# Design and Analysis of Lightweight Trust Mechanism for Secret Data using Lightweight Cryptographic Primitives in MANETs

Adarsh Kumar[1], Krishna Gopal[1], and Alok Aggarwal[2]
*(Corresponding author: Adarsh Kumar)*
Computer Science Engineering and Information Technology Department, Jaypee Institute of Information Technology[1]
A-10, Sector-62, Noida, India
(Email: adarsh.kumar@jiit.ac.in)
JP Institute of Engineering and Technology, Meerut[2]
Mawana Road, P.O. RAJPURA, Rajpura Meerut, Uttar Pradesh, India
*(Received May 17, 2013; revised and accepted Apr. 20 & Nov. 6, 2014)*

## Abstract

Lightweight trust mechanism with lightweight cryptography primitives and post-quantum cryptosystems are having important concerns in resource constraint wireless sensor based Mobile Ad Hoc Networks (MANETs). In post-quantum cryptosystems, error correcting codes (ECC) help in code based cryptography for lightweight identification, authentication, distance bounding and tag with ownership transfer protocols to provide security. In this work, a novel approach is designed to secure the RFID-Sensor based MANET that uses ECC for assigning identification to resource constrained mobile nodes. This assignment helps to create centralized environment with subgroups, groups and hierarchies. Group or subgroups boundaries are limited through distance bounding protocols. Trust management plays the role of maintaining the relationship between nodes for long endeavor. Probability analysis of distance bounding protocol shows that the proposed approach is protected from mafia fraud, distance fraud, terrorist fraud, and distance hijacking attacks. The success of these attacks on the proposed mechanism dependence on trust score: lesser trust score ($\leq 50$) increases the chances of these attacks whereas higher trust score protects the network from these attacks and improves the network performance as well. In performance analysis, it is observed that the Zone Routing Protocol (ZRP) outperforms the other MANET routing protocols in terms of network performance and security for the proposed scheme. However, the probabilistic analysis proves that it is still possible to control outliers in the network despite the new inserted defenses with trust management and limited resources.

*Keywords: MANET, RFID, zone routing protocol*

## 1 Introduction

Radio frequency identification (RFID) devices are the low cost computing devices for automatic identification, locating and tracking objects using radio frequency (RF). RFID networks are having many applications like: access rights, object tracking, inventory management, library management etc. RFID devices are classified into three major components: tag, reader and back-end system. Tag includes the identification mark and a small memory unit to store information about product, object or environment. Reader helps to write and/or read information to tag. The read information is delivered to backend system for storage, migration etc. Wireless sensor networks (WSNs) and RFIDs are the two complementary technologies. WSNs consist of small sensing devices with wireless communication medium. In compliment to RFID, WSNs consist of multi-hop, smart sensing, tracking and reprogrammable devices. However, integration of WSNs and RFIDs provides sensors to read tags, intelligence, sensing, ad-hoc and wireless communication facilities. These facilities result in many advantages which include: network-resource-data expandability, network-information scalability, portable readers extendability for speeding the on spot and random data collection, reducing hardware cost etc. [45, 74]. Requirements to integrate RFID-sensor network include accurate and reliable communication, energy efficiency and network maintenance [19, 74]. Various proposals are given to integrate RFID and sensor networks. In [72, 74], three types of integration mechanisms are proposed. In first integration mechanism, RFID tags are integrated with sensor devices. In this mechanism, two approaches are suggested to integrate RFID tags and sensors. In first approach, tags are integrated with sensor devices and communicate only with readers. Second approach suggest to integrate tag with

sensor devices and they communicate with each other to construct an ad hoc network. In second integration mechanism, reader are integrated with sensor devices [24, 74]. In this mechanism, readers attached with sensors collect data from RFID tags. Readers-sensor attachment communicates to route the information and construct an ad hoc network. In [26], a commercial solution to integrate RFID and mobile devices is proposed. This solution helps to construct MANET. In third integration mechanism, a mixed architecture is proposed. In this architecture, tags and sensor nodes are kept independent but coexist in same network. Mixed architecture consist of smart stations, RFID tags and sensor nodes. Smart stations are composed of RFID reader, a microprocessor and a network interface. Both RFID and Sensor networks are pervasive networks and require more attention on all aspects of its security. Security aspects in these networks include access rights, identification, authentication, authorization, ownership transfer, hardware cryptographic implementation, message delivery guarantee, security threats, tampering, forging etc. [5, 40]. Among WSNs, security and privacy issues include physical attacks, jamming, tampering at physical layer, packet disruption and collision at data link layer, spoofing, sybil, altering, replaying, wormhole and sinkhole attacks at network layer, flooding at transport layer, cloning, incorrect location reference, data aggregation, time synchronization and masquerading attacks in service and application layer. Among RFIDs, security and privacy issues include spoofing, cloning, tampering, tracking, denial of service, etc. [62]. Solutions to these security and privacy issues are achievable through cryptography or detection and prevention mechanisms [62]. Cryptography is an art of writing or solving the codes which is classified into symmetric and asymmetric cryptosystem.

Asymmetric cryptosystem is considered to be more secure than symmetric cryptosystem. In asymmetric cryptosystem, key can be easily shared between two parties without the need to pre-establish any key. But algorithms of asymmetric cryptosystem can be easily broken using quantum computers [58]. Thus, Elliptic Curve Cryptosystem (ECCr), ElGamal Cryptosystem, RSA, etc. are not considered to be secure against quantum computers [14]. Hence demand of designing secure system increases and it results to post quantum cryptosystem [51]. Post quantum cryptosystem can be classified as: Hash based, Lattice based, Coding based, Multivariate-quadratic and Secret key cryptosystem [11]. These systems are considered to be secure against quantum computers. Both RFID and sensor based Mobile Ad Hoc Networks (MANETs) are resource constraint devices and thus require lightweight cryptographic primitives. These lightweight cryptographic aspects should be accommodated within one third of the total hardware available. This space may increase three to four times at lesser cost in future [76]. Lightweight hierarchical error correcting codes are an efficient approach for node interconnection in resource constraint devices [10]. Such hierarchical systems decrease the losses, errors, noises, implementation overhead and improve performance, throughput, goodput, etc. In order to achieve complete security, lightweight cryptographic primitives can be integrated with hierarchical distribution for achieving the necessary performance and security.

For achieving complete system security, a three dimensional McCumber Cubes model suggests various cryptographic primitives: transmission, storage, processing, confidentiality, integrity, availability, human factor, policy with practices and technology [47]. During these phases various aspects are taken into consideration like: user rights and roles, usage policies, trust policies, password policy, authentication policy, security policies, educating security policy, training policies, privacy rights, etc. Trust management is an important aspect of consideration. Trust is a behavior assessment and it is defined in many ways [4, 22, 23, 33, 46, 48, 64]. Trust can be measured based on various aspects like: integrity, ability and benevolence, key generation, identification, information secrecy, simulator aspects, etc. [32, 69]. In this work trust is used to establish and maintain relationships between nodes.

The current study proceeds as follows. Section 2 provides background on lightweight cryptographic primitives, protocols and trust management. Section 3 introduces the assumption and premises used in this work. In section 4, proposed method for integrating lightweight identification, lightweight authentication, lightweight distance bounding, lightweight tag and ownership transferred is presented using lightweight trust management mechanism. Section 5 describes the probability based attack analysis in distance bounding protocols. Simulation and protocol policy analysis of proposed hierarchical network is also presented in section 5. Finally, section 6 concludes the work.

## 2 Background

Lightweight cryptography is classified as: lightweight primitives and lightweight protocols [2]. Two major classes of lightweight primitives are: symmetric and asymmetric primitives. Symmetric primitives include block cipher, stream cipher, hash function, pseudo random number generation and asymmetric primitives include number based system, discrete logarithmic construction and curve based cryptosystem. Lightweight Protocols can be classified as: identification, authentication, distance bounding, yoking, tag ownership protocols, etc. In resource constraint devices, upto 30% of gate equivalents (GEs) are available for lightweight cryptographic primitives and protocols [34, 53]. These GEs can increase with advancement of technology [49].

On radio frequency signal, authenticity and validity of users and messages is achieved through cryptographic primitives, ultra-lightweight operations, EPC-global Class1 Generation2 protocols, physical primitives, etc. [2]. Unique serial number generation [35, 41, 44, 65]

and plausibility check [44, 52] are the authentication mechanisms without using tags. These protocols are application dependent solutions for authentication with proper justification. A leak in justification enhances the chance of un-authenticated users become part of network. Authentication solutions through cryptography avoid cloning. For example: encryption/decryption, hash-lock, hash based synchronous secret, Hopper and Blum (HB), pseudo random number based protocols, zero knowledge device authentication, etc. are cryptography mechanisms for providing authentication [44]. In another solution [50], physical properties of product stores the unique and cryptography based data for avoiding counterfeiting and un-authorized access. Apart solutions from cryptography, specific security model based requirements for authentication is considered to be a valid choice [13]. Among these protocols, traceability, de-synchronization, man-in-middle, cracking codes using basic binary operation, etc. are commonly found to be the attacks [6, 15, 61]. Cryptography based authentication solutions are costlier also. For example, although hash based solution are found to be perfect in security but the hardware cost for implementing a hash based solution proposed is almost infeasible solution [60]. Hash based solutions like: RIP, RAP, O-RAP, O-RAKE, etc. easily avoids the traceability attacks. Cryptography based stored information containing unique identification, anonymity and anti-cloning mechanism provides maximum security through hashing only [12]. In [3], it is found that computational workload and scalability are the major challenges in hash based schemes. However, solutions has been proposed to increased the scalability and security of authentication protocols through hashing. For example, Avoine mutual authentication protocol is a two phase hash based mechanism and it is designed to increase the scalability and security. Here, scalability is limited with distance bounding and removal of distance based frauds.In lightweight cryptography, various solutions for lightweight authentication protocols are proposed. For example, Lightweight Mutual Authentication protocol (LMAP) [67]. LMAP provides security against replay, forgery, anonymity, etc. However, this protocol is not secure against traceability attack. Protocol for Lightweight Authentication of IDentity (PLAID) provides authentication and enhances the privacy through confidentiality and integrity [9]. This solution is designed for contactless smart card systems. Efficiency and reduction of costs are the real advantages of this protocol. It also provides fast and strong security between smart card and terminal devices. Strong security is achieved by not leaking the identity information.

Trust Management involves trust measurement, trust propagation, trust accumulation, trust prediction and trust application [20, 28, 29]. Trust measurement is a subjective calculation that one node has to establish on another. Trust measurement among various nodes of a resource constraint network is another challenge. CuboidTrust is a positive or negative signal based global trust computational method [18]. This method also helps to determine quality and contribution of nodes in a network. EigenTrust is satisfactory or unsatisfactory transaction based method with malicious node identification [36].

Health of resource constraint mobile nodes plays an important role in measuring the trust score. In this work, health is measured with the help of three components: lightweight energy measurements, lightweight route acting algorithms and lightweight vibration signals. Lightweight energy conservation and measurement algorithms in lightweight mobile sensor networks with ability of full coverage play an important role in trust computation. Energy in ad hoc networks is consumed through three modes: transmitting, receiving or simply "on" [25]. Saving energy increases the lifetime and utilization of ad hoc nodes. Transmitting data is major source of energy consumption among three components [25]. Receiving or collecting information is divided into four major components: discovery, data transfer, routing and motion control [27]. Discovery information can be collected from either of the two methods: Mobility independent protocols or knowledge based protocols. Mobility independent protocols are further classified into three schemes: scheduled rendezvous, on-demand and asynchronous [27]. Schedules based protocols classification involve time slot, frequency based and spread spectrum codes [75]. In these types of networks, slots are fixed for every node thus no chance of collision or overhead, easy to implement and energy efficient but assigning numbers to nodes for specific slot can prolonged delay. For example, Chakrabarti et. al. proposed a wake up mechanism on time schedule [17]. Zhang et. al. proposed ZebraNet based on global positioning system (GPS) and derivation of schedule mechanism [73]. Other examples of scheduling based protocols developed for sensor nodes are: TRAMA [56], FLAMA [55], SMACS [59], SRSA [68], R-MAC [71], DW-MAC [62, 75], etc. On-demand protocols are based on wakeup calls. Whenever some event signals to channel, it intimates to the sensor node and that node power up the data radio and start transmission. In this type of protocols, two types of signals are required to complete the process: one for wakeup call and second for data transmission. Various mechanisms are used to complete this functionality. Wakeup call could be performed using low frequency and data transmission through high frequency [57], wakeup call and data transmission call are performed using separate messages [70].

# 3 Proposed Scheme

Table 1 shows the symbols used in this work.

## 3.1 Lightweight Identification

In order to reduce the computation cost, Reed-Muller codes is used for identifying the tags. $BC_{2^n}^{M_{(c,d)}^{(a,b)}}$

Table 1: Symbols

| Symbol | Quantity |
|---|---|
| $M_{(c,d)}^{(a,b)}$ | $c^{th}$ mobile node in $d_{th}$ subgroup at $a^{th}$ layer with $b^{th}$ network. Here, $a, b, c, d \epsilon \{1, 2...\infty\}$. |
| $BC_{2^n}^{M_{(c,d)}^{(a,b)}}$ | binary code selected for $M_{(c,d)}^{(a,b)}$. |
| $SM_{(e,d)}^{HL_a}$ | $e^{th}$ subgroup member in $d^{th}$ subgroup at $a^{th}$ layer. |
| $CW_{BC_{2^n}^{M_{(c,d)}^{(a,b)}}}$ | codeword generated with length $L$ and distance $D$. |
| $SG_d^{HL_a}$ | $d^{th}$ subgroup at $a^{th}$ layer. Selection of $SG_d^{HL_a}$ is based on HEALTH, i.e. $HEH^{MN_a}$. |
| $HEH^{MN_a}$ | HEALTH,$HEH^{MN_a} \epsilon f\{ES^{M_a}, RAS^{M_a}, VIB_+^{SM_{(e,d)}^{HL_a}}\}$. |
| $ES^{MN_a}$ | energy state |
| $RAS^{MN_a}$ | router acting strength moment |
| $VIB_+^{SM_{(e,d)}^{HL_a}}/VIB_-^{SM_{(e,d)}^{HL_a}}$ | positive/negative vibration signals send from subgroup member |
| $PS^{MN_a}$ | $a^{th}$ mobile node in its full energy and without being attacked |
| $SG_{SC_d^{HL_a}}$ | subgroup controller of $d^{th}$ subgroup at hierarchical layer $HL_a$ |

is an ary code with elements $(CW_{BC_{2^n}^{M_{(c,d)}^{(a,b)}}}, L, D)$. A new binary code for next node is generated as $BC(m)_{2^n}^{M_{(c,d)}^{(a,b)}} = BC(m_1)_{2^n}^{M_{(c,d)}^{(a,b)}} * BC(m_2)_{2^n}^{M_{(c,d)}^{(a,b)}} = \{(X, X + Y), X \epsilon BC(m_1)_{2^n}^{M_{(c,d)}^{(a,b)}}$ and $Y \epsilon BC(m_2)_{2^n}^{M_{(c,d)}^{(a,b)}}\}$. Major strengths of this coding technique are: (i) with the help of small key size it provides strong security, (ii) it reduces the probability of cheating some node to a great extent and (iii) computational complexity is very less. Weakness of this coding technique is that it is prone to structural attack.

## 3.2 Lightweight Grouping

Trust management plays an important role for forming secure local subgroups for information exchange. It is also necessary to integrate additional trust security layer to resource constraint sensor nodes since cryptographic primitives do not provide complete security and any extra computation is not feasible on these nodes [37]. In order to compute trust, following steps are followed: (a) gather node information, (b) propagate information, (c) map to trust model and make trust decision [37].

### 3.2.1 Gather Node Information

Taarget node's reliability for information transfer can easily be calculated through neighboring nodes. Neighbor node can send $VIB_+^{SM_{(e,d)}^{HL_a}}$ or $VIB_-^{SM_{(e,d)}^{HL_a}}$ signal towards $SM_{(e,d)}^{HL_a}$. Strength of signal can be calculated through different ways such as: forwarded packets, intentionally dropped packets, intentionally forward packet through some legitimate intermediate node, impersonation or masquerading of data to bogus data, probability of some event, etc. Probability of finding an anomaly in attending or reporting in a regular event is helpful for providing neighboring node information [43]. Now, probability of following a path from source $(SR^{(x_1,y_1)})$ to destination $(DT^{(x_n,y_n)})$ is identified using Markov chain. $P(SR_1^{(x_1,y_1)}, SR_2^{(x_2,y_2)}, SR_3^{(x_3,y_3)}.DT_n^{(x_n,y_n)}) = P(SR_1^{(x_1,y_1)} = SR_1^{(x_1,y_1)} * p_{x_1x_2} * p_{x_2x_3}..... * p_{x_{n-1}x_n} = P_S$, i.e. when probability reaches zero then that particular region is called an event region. When a node follows a particular path, Frisbee model [16] is used to construct subgroups. This model in resource constraint network reduces losses. Figure 1 shows the construction of Frisbees with fixed number of nodes. In the process of creating single-hop Frisbees, node communicates with other node through lightweight and energy efficient authentication mechanism.

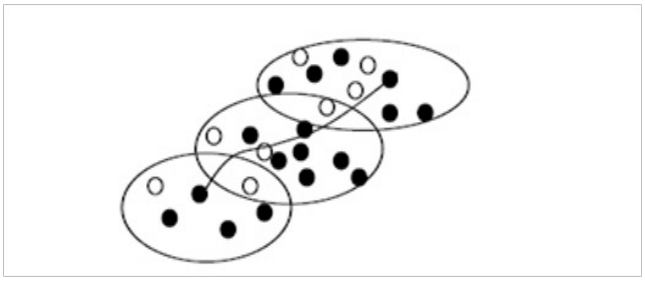

Figure 1: Frisbee construction with mobility of node

### 3.2.2 Propagate Information

Once subgroups are constructed then these subgroups are merged to form hierarchy. Each $SG_{M_{(c,d)}^{(a,b)}}^{HL_i}$ at every hierarchical layer will contain a subgroup controller. Figure 2 shows the construction of hierarchy with movement of $M_{(c,d)}^{(a,b)}$ that may take the form of $SG_{SC_d}^{HL_i}$. As shown in Figure 2, $M_{(c,d)}^{(a,b)}$ will act as producer $(P_i)$ or consumer

($C_i^{'}$ or $C_i^{''}$). These producer and consumer will perform multiple tasks like: (i) distribution of $BC(m_1)_{2^n}^{M_{(c,d)}^{(a,b)}}$, (ii) with the help of $BC(m)_{2^n}^{M_{(c,d)}^{(a,b)}}, SG_{SC_d}^{HL_i}$ generate keys and distribute to consumers and (iii) nodes exchange messages using lightweight encryption mechanism.

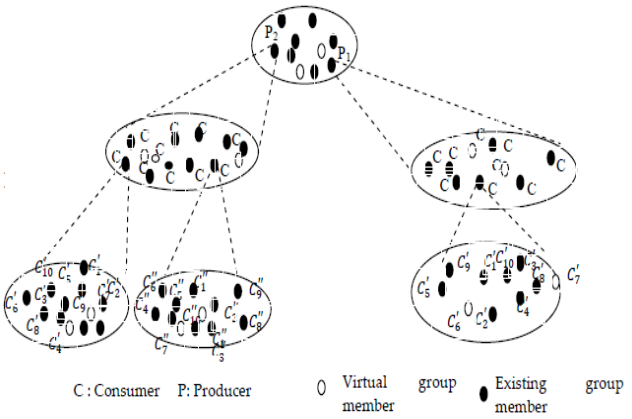


Figure 2: Hierarchical formation using real and virtual nodes

- During distribution of $BC(m)_{2^n}^{M_{(c,d)}^{(a,b)}}, P_i$ will fetch the reed-muller binary code from the database and distribute to $C_i^{'}$ or $C_i^{''}$. The producer-consumer module to exchange reed-muller code using interface, port and channel is shown in Figure 3. Here, n-consumer modules are connected to single producer and each producer/consumer module is associated with an interface. These are writing and reading interfaces at producer and consumer ends respectively. Since producers generate and consumers accept reed-muller codes thus port associated with producer is output and consumer is input.

- With the help of $BC(m)_{2^n}^{M_{(c,d)}^{(a,b)}}, SG_{SC_d}^{HL_i}$ generate keys and distribute to consumers. In [42], efficient hierarchical threshold based symmetric group key management protocol is proposed. It is found that inclusion of virtual nodes reduces the energy losses and joining/leaving expenses of nodes. Extension to Teo and Tan's group key management protocol is integrated to generate and distribute a group symmetric key '$K'$ [42, 66]. Major strengths of this process are: (i) protected from forward and backward secrecy, (ii) strong authentication mechanism and (iii) efficient in terms of small subgroup formation in close vicinity.

- With help of symmetric key '$K'$, messages are exchanged using protocol1 between smart nodes. Here, smart node is integration of RFID reader with mobile sensor node. Reader reads the information from nearby tags and communicates to other sensor nodes through radio frequency. A microcontroller is used to make the RFID reader data compatible for sensor node in a smart node.

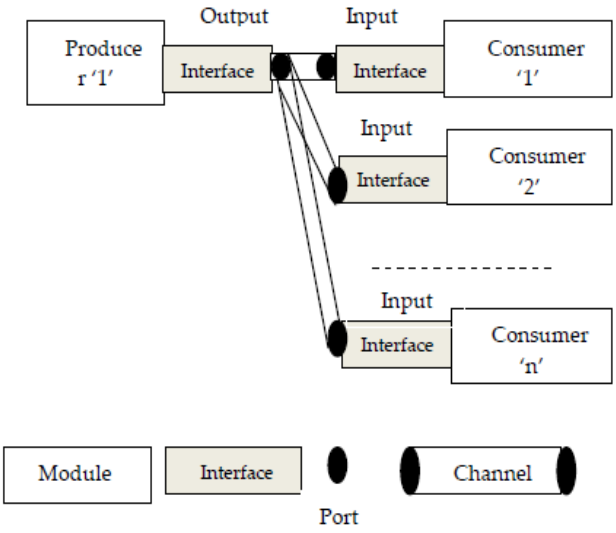


Figure 3: Exchange of $BC(m)_{2^n}^{M_{(c,d)}^{(a,b)}}, P_i$ using producer-consumer

**Protocol 1:** Messages exchange using lightweight encryption/decryption mechanisms.
**Premise:** Let $E_K, D_K$ and $H$ represents the lightweight encryption, decryption and hashing functions respectively.

1) $SG_{SM_j}^{HL_i} \rightarrow SG_{SM_r}^{HL_o} : \{E_K\{Message\}, H(Message)\}$.

2) $SG_{SM_r}^{HL_o}$ verifies the message digest by regenerating it using $H(D_K(E_K\{Message\}))$. If $H(D_K(E_K\{Message\})) = H(Message)$ then message is accepted otherwise rejected.

3) if message is accepted then $SG_{SM_r}^{HL_o} \rightarrow SG_{SM_j}^{HL_i}$: $\{E_K\{Acknowledgement\}, H(Acknowledgement)\}$ and if message is rejected then $SG_{SM_r}^{HL_o} \rightarrow SG_{SM_j}^{HL_i}$: $\{E_K\{Negative\_Acknowledgement\}, H(Negative\_Acknowledgement)\}$.

4) $SG_{SM_j}^{HL_i}$ verifies the receipt of message through acknowledgement as: $H(D_K(E_K\{Acknowledgement\}))$.
If $H(D_K(E_K\{Acknowledgement\})) = H(Acknowledgement)$ then message is accepted otherwise retransmission start with timer.

These steps of message exchange ensures: (i) confidentiality of message exchange through encryption/decryption, (ii) message integrity through lightweight hashing hashing, (iii) pre-image resistant and collision resistant properties of messages through lightweight hashing, (iv) compression of message through hashing and (v) retransmission of messages in case of message loss or corruption.

#### 3.2.3 Map to Trust Model

As discussed, trust management includes trust generation, trust propagation, trust accumulation, trust prediction and trust application [29]. Once subgroup is constructed using protocol1 then it can be protected from various attacks and maintains the relationships using trust management. Trust mechanism assumes every member of constructed hierarchy as $PS^{MN_a}$ and passes through following phases for maintaining relationships.

**Trust Generation:** Trust on a mobile node is calculated from its $HEH^{MN_a}$ score. Trust is directly proportional to $HEH^{MN_a}$ score. Initially, all nodes are considered to be $PS^{MN_a}$ and vibrate $VIB_{+}^{SM_{(e,d)}^{HL_a}}$ signal only. Here, health is calculated from three factors i.e. $HEH^{MN_a} \epsilon f\{ES^{M_a}, RAS^{M_a}, VIB_{+}^{SM_{(e,d)}^{HL_a}}\}$. Three component's values are rated on grading scheme in order to calculate the trust value of any node and this grading process is explained as follows:

- $RAS^{M_a}$ ensures reliability and quality of service. Since all nodes are considered to be $PS^{MN_a}$ thus reliability and quality of nodes is assumed to be very high. Reliability of node is dependent upon delivery ratio, goodput, coverage, fairness, jitter and routing cost [54]. Quality of service is calculated from number and type of interactions, which is calculated as probability score value (PSV) and it is calculated as number of times the $P(SR_1^{(x_1,y_1)}, SR_2^{(x_2,y_2)}, SR_3^{(x_3,y_3)} \cdots DT_n^{(x_n,y_n)})$ of any $M_{(c,d)}^{(a,b)}$ reaches zero in some region 'R'. Interactions in this region may transmit very good, good, average, poor or very poor quality of transmissions.

- $ES^{M_a}$ is measured in form of bursts and sleep time. These bursts are scaled based on traffic. Low traffic consumes less energy and heavy traffic consumes high energy. In order to rate energy levels, bursts are divided into four major categories: zero, low, medium and high. Zero bursts do not consume energy and in this state, nodes are assumed to be in sleep state. Low bursts are the minimum consumption states. Medium bursts are the frequent consumption states but do not increase its value with time as compared to high bursts which are more frequent. Energy consumption increases with time if high bursts are contineously observed. Section 5 describes the energy consumption analysis.

- $VIB_{+}^{SM_{(e,d)}^{HL_a}}$ are the positive vibration signals and present experiences of neighboring nodes. A node can send positive or negative vibration signals. Positive signals are used to indicate trust and negative for un-trust. In this work, counts on positive signals are made to measure the trust. This count value ranges from 1(Low) to 10 (High). Rating is the number of trust response coming from neighboring nodes. If number of neighboring nodes exceed ten then it is considered to be highly trusted but if number of neighboring nodes response is less than ten then 10 minus total response will give negative vibration score. Subgroup signal value is also calculated from the average score of it's node's trust vibration scores. Subgroup controller can debar any subgroup from hierarchy because of its malicious operations. Which is calculated from its subgroup members health score.

Table 2: Lightweight automatic trust propagation-intruder analysis (time in msec)

| Percentage age of SCORE ($HEH_{neighbor}^{MN_a}$) | Intruder Assertions | Proposed Trusted Strategy | |
|---|---|---|---|
| | | Time (Steps) | Result |
| More than 90 | 1/5/10 | 20/21/26 (120/226/351) | Proved |
| 90 to 75 | 1/5/10 | 35/42/61 (222/350/595) | Proved |
| 75 to 60 | 1/5/10 | 41/61/74 (332/530/650) | Proved |
| 60 to 45 | 1/5/10 | 52/74/85 (436/626/751) | Proved |
| Less than 45 | 1/5/10 | 62/84/95 (546/726/881) | Proved |

**Trust Propagation:** Once trust of node is calculated then its value is propagated to other nodes. This propagation is made through selective algorithm [63]. Range of $SCORE(HEH_{neighbor}^{MN_a})$ selected for selective algorithm is analyzed using Alloy [30, 31]. Alloy is a lightweight, powerful, simple design, automatic and animation analysis tool. Table 2 shows that there are five ranges of health score: more than 90, 90 to 75, 75 to 60, 60 to 45 and less than 45. There are three variations of intruders: 1, 5 and 10 to analyze the proposed mechanism. This analysis shows that with change in every score range, there is an increase in minimum of 10 msec and 100 steps to detect intruders. However, intruders are detectable and results are proved in this tool. According to selective algorithm, single high health score neighbor is selected if $SCORE(HEH_{neighbor}^{MN_a}) \geq 90\%$, two high score neighbor are selected if $90\% \gtrsim SCORE(HEH_{neighbor}^{MN_a}) \geq 75\%$ ,three high score neighbor are selected if $75\% \gtrsim SCORE(HEH_{neighbor}^{MN_a}) \geq 60\%$, four high score neighbor are selected if $60\% \gtrsim SCORE(HEH_{neighbor}^{MN_a}) \geq 45\%$, transmit to all neighboring nodes if $45\% SCORE(HEH_{neighbor}^{MN_a})$. Multiple entities of trust are re-evaluated in trust prediction phase through identification marks since each communication contains its identification, i.e. $BC(m)_{2^n}^{M_{(c,d)}^{(a,b)}}) \parallel SCORE(HEH_{neighbor}^{MN_a})$. This mechanism of trust propa-

gation through health score help in protecting the network from various attacks.

Table 3: Lightweight automatic trust accumulation-intruder analysis (time in msec)

| Percentage age of SCORE ($HEH_{AVG}$) | Intruder Assertions | Proposed Trusted Strategy | |
|---|---|---|---|
| | | Time (Steps) | Result |
| More than 90 | 1/5/10 | 31/41/44 (131/233/362) | Proved |
| 90 to 80 | 1/5/10 | 42/52/71 (222/362/493) | Proved |
| 80 to 70 | 1/5/10 | 54/61/88 (341/466/645) | Proved |
| 70 to 60 | 1/5/10 | 64/81/101 (531/771/823) | Proved |
| 60 to 50 | 1/5/10 | 74/93/118 (666/902/1120) | Proved |
| Less than 50 | 1/5/10 | 92/104/165 (786/966/1481) | Proved |

**Trust Accumulation:** At destination, trust values are accumulated and evaluated. Since, trust value passes through multiple paths hence source's trust value is predicted from health of the path followed. Health of each routed node is accumulated along with its trust value. Average of health is calculated using: $HEH_{AVG} = (HEH^{MN_1} + HEH^{MN_2} + .. + HEH^{MN_n})/N$. Based on $score(HEH_{AVG})$ value, path is selected and rated. Table 3 shows that there are six range of score($HEH_{AVG}$). With decrease in $score(HEH_{AVG})$ of 10% there is an increase in minimum of 10 msec and 100 steps to detect intruders. However, intruders are detectable and results are proved on alloy tool. This measurement is taken to rate the path followed for trust accumulation. If $score(HEH_{AVG}) \geq 90\%$, then path is considered as excellent, very good if $90\% \gtrsim score(HEH_{AVG}) \geq 80\%$, good if $80\% \gtrsim score(HEH_{AVG}) \geq 70\%$, average if $70\% \gtrsim score(HEH_{AVG}) \geq 60\%$, below average if $60\% \gtrsim score(HEH_{AVG}) \geq 50\%$, poor if $50\% \gtrsim score(HEH_{AVG})$.

**Trust Prediction:** Now, after transmitting the trust score in the form of health, healthiness of route is determined. If route health is below average then trust is recomputed at destination using lightweight trust computation based on prejudice, experience and hearsay. It is calculated as: $T^i = C * Exp. + (1 - C) * Her.$, where T, C, Exp. and Her. are respectively the trust, self confidence level, experience and hearsay values. Experience is the average value of current observation and immediate observation. Hearsay is calculated as: $H(MN^j) = (\Sigma_{i=1}^{n} T^i)/N$. Here, $N$ is the number of neighboring connected nodes to $MN_a$ and $T^i$ is the $i^{th}$ response of trust.

**Trust Application:** Once basic trust relationship is established then application specific trust depends upon user operations. Secure and safe transmission of information is necessary and confirmed through authentication procedures. Applications that are required to be operated in basic trusted environment should have to produce application trust value ($T_a$). This trust value is compared with basic trust value ($T_i$). If $T_a \lesssim T_i$ then access to application fails. Failure or success of the application for operation is broadcasted to other subgroup members using broadcasting mechanism. Protocol 2 describes this mechanism.

**Protocol 2:** Application trust broadcasting for access rights.
**Goal:** To compare trust value with required application trust value. After this comparison, if application trust value is less then access to application is not allowed and this information is broadcasted to all subgroup members.

1) $SG_{SM_j}^{HL_i} \rightarrow SG_{SM_k}^{HL_i}$ : "$ALLOW$" $\|$ "$DENY$".
2) $SG_{SC_k}^{HL_i} \rightarrow SG_{SC_k}^{HL_{i-1}}$ : "$ALLOW$" $\|$ "$DENY$". This step is repeated until top subgroup controller receives the message.
3) $SG_{SC_k}^{HL_o}$ initiated the process of collecting information about applications whose access rights are managed through trust comparison.

Here, ALLOW and DENY are single bit messages. These messages help to debar the applications that can maliciously harm the network. If '$h$' is the height of hierarchy constructed and '$n$' is the total number of subgroup constructed then total number of messages required to broadcast this information are '$h * n * 10$'. In this work, a set of two node based trust applications are integrated for distance bounding. This trust application is explained in next sections.

## 3.3 Lightweight Trust Based Distance Bounding and Authentication

In this section, distance bounding and authentication protocols are integrated to hierarchical model for limiting the distance between two nodes and to authenticate each other. Distance bounding and authentication are two set of protocols but an integrated form of these protocols is used to reduce the hardware cost. In this work, modified form of Avoine mutual authenticated KA2 (MA-KA2) protocol is integrated with lightweight parameters [7]. The modified form of this mechanism is explained in Protocol 3. There are two phases of protocol: slow and fast. In slow phase, nonce values are exchanged and in fast phase, authentication is performed using

challenge-verify process.

**Protocol 3:** Modified MA-KA2 and Distance Bounding Protocol.

**Premises:** Let $R^{M^{(a,b)}_{(c,d)}}$ be the random number selected by $M^{(a,b)}_{(c,d)}$.$N_{SG^{HL_a}_{SC_d}}$ represents the nonce generated by $d^{th}$ subgroup with its subgroup controller. Here, every subgroup member act as a prover or a verifier. When direction bit $DIR^i_{M^{(a,b)}_{(c,d)}}$ of some mobile node is zero then $M^{(a,b)}_{(c,d)}$ sends a random challenge $CHA^i_{M^{(a,b)}_{(c,d)}} \epsilon \{0,1\}$ towards another mobile node $M^{(a,b)}_{(f,d)}$. Now, this mobile node replies with verification process ($VER^{CHA^i}_{M^{(a,b)}_{(f,d)}}$). When $DIR^i_{M^{(a,b)}_{(c,d)}}$ is one then $M^{(a,b)}_{(f,d)}$ will send $CHA^i_{M^{(a,b)}_{(f,d)}} \epsilon \{0,1\}$ and $M^{(a,b)}_{(c,d)}$ will verify. If the random number generated is not verified, i.e. $R^{M^{(a,b)}_{(c,d)}} \neq VER^{CHA^i}_{M^{(a,b)}_{(a,d)}}$ then communication is put in protected mode. This protected mode behaves differently than regular rounds. In this mode, nodes have to regularly produce and verify the challenges. Let $b$ and $r$ are the number of bits used in direction bit and number of rounds in two phases of distance bound mutual authentication protocol. $T_{M^{(a,b)}_{(c,d)}}$ represents the timer from $M^{(a,b)}_{(c,d)}$,$T_{MAX}$ is the maximum time elapsed for checking distance bounding and $H$ is a pseudorandom number function.

**Goal:** Limit the distance between two subgroup controllers or members and authenticate each other.

**Step 1:** Slow Phase

1) Every subgroup member from both subgroups will select a random number, i.e. $R^{M^{(a,b)}_{(1,d)}}, R^{M^{(a,b)}_{(2,d)}} ... R^{M^{(a,b)}_{(9,d)}}$ and $R^{M^{(a,b)}_{(1,e)}}, R^{M^{(a,b)}_{(2,e)}} ... R^{M^{(a,b)}_{(9,e)}}$.

2) Since a symmetric key $K$ is already shared between subgroup members thus nonce are generated using: $N_{SG^{HL_a}_{SC_d}} = H(K, R^{M^{(a,b)}_{(1,d)}} \parallel R^{M^{(a,b)}_{(2,d)}} \parallel ... \parallel R^{M^{(a,b)}_{(9,d)}})$ and $N_{SG^{HL_a}_{SC_e}} = H(K, R^{M^{(a,b)}_{(1,e)}} \parallel R^{M^{(a,b)}_{(2,e)}} \parallel ... \parallel R^{M^{(a,b)}_{(9,e)}})$. Here, $H$ is a lightweight cryptographic hash function.

3) Two subgroup controller exchanges these nonce values as: $SG^{HL_a}_{SC_d} \rightarrow SG^{HL_a}_{SC_e} : N_{SG^{HL_a}_{SC_d}}, SG^{HL_a}_{SC_e} \rightarrow SG^{HL_a}_{SC_d} : N_{SG^{HL_a}_{SC_e}}, \{DIR^i_{SG^{HL_a}_{SC_d}} \parallel DIR^i_{SG^{HL_a}_{SC_e}} \parallel VER^{CHA^0} \parallel VER^{CHA^1} \parallel VER^{CHA^2}\} = h(K, N_{SG^{HL_a}_{SC_d}}, N_{SG^{HL_a}_{SC_e}}$ Number of bits $(DIR^i_{SG^{HL_a}_{SC_d}})$ = Number of bits$(DIR^i_{SG^{HL_a}_{SC_e}}) = r$, Number of bits $(VER^{CHA^0})$ $= Numberofbits(VER^{CHA^1}) = 2(b-r)-1$, Number of bits $(VER^{CHA^2}) = 2b$.

**Step 2:** Fast bit exchange phase

1) $SG^{HL_a}_{SC_d}$ computes $COM^1_{SG^{HL_a}_{SC_d}} = DIR^1_{SG^{HL_a}_{SC_d}}$ and start timer $T_{SG^{HL_a}_{SC_d}}$. During this time, it sends $COM^1_{SG^{HL_a}_{SC_d}}$ towards $SG^{HL_a}_{SC_e}$.

2) $SG^{HL_a}_{SC_e}$ checks if $COM^1_{SG^{HL_a}_{SC_d}} = DIR^1_{SG^{HL_a}_{SC_d}}$ then computes $COM^1_{SG^{HL_a}_{SC_e}} = VER^{CHA^2}_1$ . With start of $T_{SG^{HL_a}_{SC_e}}, SG^{HL_a}_{SC_e}$ sends $COM^1_{SG^{HL_a}_{SC_e}}$ to $SG^{HL_a}_{SC_d}$. But if $COM^1_{SG^{HL_a}_{SC_d}} \neq DIR^1_{SG^{HL_a}_{SC_d}}$ then error is detected and instead of sending random answers until end of the protocol it check value of $HEH^{MN_a}_{SG^{HL_a}_{SC_e}}$ and $HEH_{AVG}$. if any value is below satisfactory level then it adds the communication in protected mode.

3) $SG^{HL_a}_{SC_d}$ stops $T_{SG^{HL_a}_{SC_d}}$ and compute $DOM^{b-1}_{SG^{HL_a}_{SC_e}} = COM^{b-1}_{SG^{HL_a}_{SC_d}} \oplus VER^{CHA^2}_{2b-3}$.if $DOM^{b-1}_{SG^{HL_a}_{SC_e}} = DIR^{b-1}_{SG^{HL_a}_{SC_e}}$ then $COM^b_{SG^{HL_a}_{SC_d}} = VER^{CHA^2}_{2b-2} \oplus DIR^b_{SG^{HL_a}_{SC_d}}$. Further, if $DOM^{b-1}_{SG^{HL_a}_{SC_e}} \neq DIR^{b-1}_{SG^{HL_a}_{SC_d}}$ then again it check for $HEH^{MN_a}_{SG^{HL_a}_{SC_d}}$ and $HEH_{AVG}$. If any of these values are unsatisfactory then it adds the communication to protected mode. Also, $SG^{HL_a}_{SC_d}$ sends $COM^b_{SG^{HL_a}_{SC_d}}$ to $SG^{HL_a}_{SC_e}$ and start $T_{SG^{HL_a}_{SC_d}}$.

4) $SG^{HL_a}_{SC_e}$ stops $T_{SG^{HL_a}_{SC_e}}$ and compute $DOM^b_{SG^{HL_a}_{SC_d}} = COM^b_{SG^{HL_a}_{SC_d}} \oplus VER^{CHA^2}_{2b-2}$. If $DOM^b_{SG^{HL_a}_{SC_d}} \neq DIR^b_{SG^{HL_a}_{SC_d}}$ then $HEH^{MN_a}_{SG^{HL_a}_{SC_d}}$ and $HEH_{AVG}$ are checked before sending unsatisfactory report for protected mode. Also, $SG^{HL_a}_{SC_e}$ start $T_{SG^{HL_a}_{SC_e}}$ and send $DOM^b_{SG^{HL_a}_{SC_d}}$ to $SG^{HL_a}_{SC_d}$.

5) $SG^{HL_a}_{SC_d}$ stops $T_{SG^{HL_a}_{SC_d}}$ and compute $DOM^b_{SG^{HL_a}_{SC_e}} = DOM^b_{SG^{HL_a}_{SC_d}} \oplus VER^{CHA^2}_{2b-1}$. If $DOM^b_{SG^{HL_a}_{SC_e}} = DIR^b_{SG^{HL_a}_{SC_e}}$ then compute $COM^{b+1}_{SG^{HL_a}_{SC_d}} = VER^{CHA^2}_{2b} \oplus R^{M^{(a,b)}_{(1,d)}}$. Further, if $DOM^b_{SG^{HL_a}_{SC_e}} \neq DIR^b_{SG^{HL_a}_{SC_e}}$ then $HEH^{MN_a}_{SG^{HL_a}_{SC_d}}$ and $HEH_{AVG}$ values are checked before sending unsatisfactory report for protected mode. $SG^{HL_a}_{SC_d}$ sends $COM^{b+1}_{SG^{HL_a}_{SC_d}}$ to $SG^{HL_a}_{SC_e}$ and start $T_{SG^{HL_a}_{SC_d}}$

6) $SG^{HL_a}_{SC_e}$ stops $T_{SG^{HL_a}_{SC_e}}$ and computes $R^{M^{(a,b)}_{(1,d)}} = COM^{b+1}_{SG^{HL_a}_{SC_d}} \oplus VER^{CHA^2}_{2b-2}$. If $R^{M^{(a,b)}_{(1,d)}} = 0$ then $COM^{b+1}_{SG^{HL_a}_{SC_e}} = VER^{CHA^0} \oplus R^{M^{(a,b)}_{(1,e)}}$ else if $R^{M^{(a,b)}_{(1,d)}} =$

1 then $COM^{b+1}_{SG^{HL_a}_{SC_e}} = VER^{CHA^1} \oplus R^{M^{(a,b)}_{(1,e)}}$. Also, $SG^{HL_a}_{SC_e}$ starts $T_{SG^{HL_a}_{SC_e}}$ and sends $COM^{b+1}_{SG^{HL_a}_{SC_e}}$ to $SG^{HL_a}_{SC_d}$.

7) $SG^{HL_a}_{SC_d}$ stops $T_{SG^{HL_a}_{SC_d}}$ and computes $R^{M^{(a,b)}_{(r-b-1,e)}} = DOM^{b-1}_{SG^{HL_a}_{SC_d}} \oplus VER^{CHA^{r-b-1}}_{2r-2b-2}$. Now, if $R^{M^{(a,b)}_{(r-1,e)}} = 0$ then $DOM^{b}_{SG^{HL_a}_{SC_d}} = VER^{CHA^0_{2r-2b-1}} \oplus R^{M^{(a,b)}_{(r-b,d)}}$ else if $R^{M^{(a,b)}_{(r-1,e)}} = 1$ then $COM^{b}_{SG^{HL_a}_{SC_d}} = VER^{CHA^1}_{2r-2b-1} \oplus R^{M^{(a,b)}_{(r-b,d)}}$. Also, $SG^{HL_a}_{SC_d}$ starts $T_{SG^{HL_a}_{SC_d}}$ and sends $COM^{b}_{SG^{HL_a}_{SC_d}}$ to $SG^{HL_a}_{SC_e}$.

8) $SG^{HL_a}_{SC_e}$ stops $T_{SG^{HL_a}_{SC_e}}$ and computes $R^{M^{(a,b)}_{(r-b-1,d)}} = DOM^{b}_{SG^{HL_a}_{SC_d}} \oplus VER^{CHA^{r-b-1}}_{2r-2b-2}$. Now, if $R^{M^{(a,b)}_{(r-b,d)}} = 0$ then $COM^{b}_{SG^{HL_a}_{SC_e}} = VER^{CHA^0}_{2r-2b-1} \oplus R^{M^{(a,b)}_{(r-b,e)}}$ else if $R^{M^{(a,b)}_{(r-b,d)}} = 1$ then $COM^{b}_{SG^{HL_a}_{SC_e}} = VER^{CHA^1_{2r-2b-1}} \oplus R^{M^{(a,b)}_{(r-b,e)}}$. Also, $SG^{HL_a}_{SC_e}$ sends $COM^{b}_{SG^{HL_a}_{SC_e}}$ to $SG^{HL_a}_{SC_d}$.

9) $SG^{HL_a}_{SC_d}$ stops $T_{SG^{HL_a}_{SC_d}}$.

**Step 3:** End of fast bit exchange phase and start check for processing delay.

1) $SG^{HL_a}_{SC_d}$ checks for $H(K, R^{M^{(a,b)}_{(1,d)}} \parallel R^{M^{(a,b)}_{(2,d)}} \parallel .... \parallel R^{M^{(a,b)}_{(9,d)}}) = N_{SG^{HL_a}_{SC_d}}$ and $SG^{HL_a}_{SC_e}$ checks for $H(K, R^{M^{(a,b)}_{(1,e)}} \parallel R^{M^{(a,b)}_{(2,e)}} \parallel ... \parallel R^{M^{(a,b)}_{(9,e)}} = N_{SG^{HL_a}_{SC_e}}$. If both are true and time elapsed is less than $T_{MAX}$ then communication is successful.

Major strengths of this protocol are: (i) one subgroup controller or member can put distance limit to another subgroup controller or member, (ii) unilateral authentication is provided to protect against dismantling attack, (iii) distance bounding protocols protects from location based attacks using cryptographic characteristics integrated with physical attributes of the nodes and (iv) attack analysis in section 5 shows that the modified protocol is efficient, secure and having lowest False Acceptance Rate (FAR). The FAR is the rate of possibility of acceptance of nodes when there are chances of attack.

# 4 Result Analysis

## 4.1 Attack Analysis

### 4.1.1 Distance Bounding Protocol Attack Analysis

In this section, probability of success of mafia fraud, distance fraud, terrorist fraud and distance hijacking attacks are analyzed on distance bounding protocols. The analysis is explained as follows:

**Attack:** Mafia Fraud Attack

**Description:** In this attack, a malicious subgroup controller ($MSG^{HL_a}_{M^{(a,b)}_{(c,d)}}$) and a malicious group member ($MM^{(a,b)}_{(c,d)}$) are inserted in subgroups. These malicious entities communicate with original subgroup controller and members and convince them to reveal secret information [59, 68, 71]. $MSG^{HL_a}_{M^{(a,b)}_{(c,d)}}$ and $MM^{(a,b)}_{(c,d)}$ start man-in-middle attack by sending $MSG^{HL_a}_{SC_d} \rightarrow SG^{HL_a}_{SC_e} : N_{MSG^{HL_a}_{SC_d}}$ and $MSG^{HL_a}_{SC_e} \rightarrow SG^{HL_a}_{SC_d} : N_{MSG^{HL_a}_{SC_e}}$. This effects the rounds of fast bit exchange. Now, success probability of this attack is determined by defining the following events:

- $AND^{i}_{SG^{HL_a}_{SC_d}}$ attack is not detected at $i^{th}$ round by $SG^{HL_a}_{SC_d}$.
- $AD^{i}_{SG^{HL_a}_{SC_d}}$ attack is detected at $i_{th}$ round by $SG^{HL_a}_{SC_d}$.
- $HEH\_AND^{MN_a}_{SG^{HL_a}_{SC_d}}$ health score of $SG^{HL_a}_{SC_d}$ at time when attack is not detected at $i^{th}$ round by $SG^{HL_a}_{SC_d}$.
- $UAND^{i}_{SG^{HL_a}_{SC_d}}$ attack is not detected at until the $i^{th}$ round by $SG^{HL_a}_{SC_d}$.
- $AND^{i}_{SG^{HL_a}_{SC_e}}$ attack is not detected at $i^{th}$ round by $SG^{HL_a}_{SC_e}$.
- $AD^{i}_{SG^{HL_a}_{SC_e}}$ attack is detected at $i_{th}$ round by $SG^{HL_a}_{SC_e}$.
- $HEH\_AND^{MN_a}_{SG^{HL_a}_{SC_e}}$ health score of $SG^{HL_a}_{SC_e}$ at time when attack is not detected at $i^{th}$ round by $SG^{HL_a}_{SC_e}$.
- $UAND^{i}_{SG^{HL_a}_{SC_e}}$ attack is not detected at until the $i^{th}$ round by $SG^{HL_a}_{SC_e}$.
- $COL^{i}_{SG^{HL_a}_{SC_d}}$ is an event when collision occurs at $SG^{HL_a}_{SC_d}$ side in $i^{th}$ round.
- $COL^{i}_{SG^{HL_a}_{SC_e}}$ is an event when collision occurs at $SG^{HL_a}_{SC_e}$ side in $i^{th}$ round.

Now, success probability of Mafia fraud attack can be calculates as follows:

$$\begin{aligned} & P[FAR] \\ = \; & P[UAND^i_{SG^{HL_a}_{SC_d}}/UAND^i_{SG^{HL_a}_{SC_e}}]P[UAND^i_{SG^{HL_a}_{SC_e}}] \\ & + \sum_{i=1}^{n} P[UAND^i_{SG^{HL_a}_{SC_e}}/AD^i_{SG^{HL_a}_{SC_d}}]P[AD^i_{SG^{HL_a}_{SC_d}}] \\ & + \sum_{i=1}^{n} P[UAND^i_{SG^{HL_a}_{SC_d}}/AD^i_{SG^{HL_a}_{SC_e}}]P[AD^i_{SG^{HL_a}_{SC_e}}] \end{aligned} \tag{1}$$

$$\begin{aligned} & P[UAND^i_{SG^{HL_a}_{SC_e}}/AD^i_{SG^{HL_a}_{SC_d}}]P[AD^i_{SG^{HL_a}_{SC_d}}] \\ = \; & \Pi_{j=1}^{i-1} P[\frac{UAND^i_{SG^{HL_a}_{SC_e}}}{AND^i_{SG^{HL_a}_{SC_d}}}]_{HEH\_AND^{MN_a}_{SG^{HL_a}_{SC_d}}=satisfactory} \\ & \Pi_{j=1}^{i-1} P[\frac{UAND^i_{SG^{HL_a}_{SC_e}}}{AD^i_{SG^{HL_a}_{SC_d}}}]_{HEH\_AND^{MN_a}_{SG^{HL_a}_{SC_d}}=satisfactory} \end{aligned} \tag{2}$$

Now, there are five case when $HEH\_AND^{MN_a}_{SG^{HL_a}_{SC_d}} = satisfactory$. Let $\frac{1}{p_{90}}, \frac{1}{p_{80}}, \frac{1}{p_{70}}, \frac{1}{p_{60}}$ and $\frac{1}{p_{50}}$ are the five case probabilities when $HEH\_AND^{MN_a}_{SG^{HL_a}_{SC_d}} \geq 90\%$, $HEH\_AND^{MN_a}_{SG^{HL_a}_{SC_d}} \geq 80\%$, $HEH\_AND^{MN_a}_{SG^{HL_a}_{SC_d}} \geq 70\%$, $HEH\_AND^{MN_a}_{SG^{HL_a}_{SC_d}} \geq 60\%$,and $HEH\_AND^{MN_a}_{SG^{HL_a}_{SC_d}} \geq 50\%$ respectively. If $\frac{1}{p_{i-1}}$ be the probability that collision is not detected until $(i-1)^{th}$ round and $\frac{1}{p_{protected}}$ is the probability of moving to protected mode then:

$$\begin{aligned} & \Pi_{j=1}^{i-1} P[\frac{UAND^i_{SG^{HL_a}_{SC_e}}}{AND^i_{SG^{HL_a}_{SC_d}}}]_{HEH\_AND^{MN_a}_{SG^{HL_a}_{SC_d}}=satisfactory} \\ = \; & (\frac{1}{p_{j-1}})^{j-1}(\frac{1}{p_{protected}})^{j-1} \\ & +(\frac{1}{p_{90}}+\frac{1}{p_{80}}+\frac{1}{p_{70}}+\frac{1}{p_{60}}+\frac{1}{p_{50}})^{j-1}. \end{aligned}$$

Thus Equation (2) can be written as:

$$\begin{aligned} & P[UAND^i_{SG^{HL_a}_{SC_e}}/AD^i_{SG^{HL_a}_{SC_d}}]P[AND^i_{SG^{HL_a}_{SC_d}}] \\ = \; & (\frac{1}{p_{i-1}})^{i-2}(\frac{1}{p_{protected}})^{i-2} \\ & +(\frac{1}{p_{90}}+\frac{1}{p_{80}}+\frac{1}{p_{70}}+\frac{1}{p_{60}}+\frac{1}{p_{50}})^{i}. \end{aligned} \tag{3}$$

Similarly,

$$\begin{aligned} & \sum_{i=1}^{n} P[UAND^i_{SG^{HL_a}_{SC_d}}/AD^i_{SG^{HL_a}_{SC_e}}]P[AD^i_{SG^{HL_a}_{SC_e}}] \\ = \; & (\frac{1}{p_{i-1}})^{i-2}(\frac{1}{p_{protected}})^{i-2} \\ & +(\frac{1}{p_{90}}+\frac{1}{p_{80}}+\frac{1}{p_{70}}+\frac{1}{p_{60}}+\frac{1}{p_{50}})^{i}. \end{aligned} \tag{4}$$

From Equations (3) and (4), one of the equation is used to find error thus it reduces the probability of finding a collision to be $\frac{1}{2}$. After putting values of Equations (3) and (4) in (2), probability of false acceptance rate can be calculated as:

$$\begin{aligned} P[FAR_n] \; = \; & (\frac{1}{p_{i-1}})^{n}(\frac{1}{p_{protected}})^{n} \\ & +(\frac{1}{p_{90}}+\frac{1}{p_{80}}+\frac{1}{p_{70}}+\frac{1}{p_{60}}+\frac{1}{p_{50}})^{n} \\ & +\sum_{i=1}^{n}((\frac{1}{p_{i-1}})^{n-i-2}(\frac{1}{p_{protected}})^{n-i-2} \\ & +(\frac{1}{p_{90}}+\frac{1}{p_{80}}+\frac{1}{p_{70}}+\frac{1}{p_{60}}+\frac{1}{p_{50}})^{n-i-2}). \end{aligned} \tag{5}$$

Equation (5) gives the false acceptance probability. Higher value of this probability give less protection against intruders at earlier stage. However, progression of relationship through trust decreases the probability and increases the security of network for finding an attack. If health score does not permit to accept any subgroup controller or member then collision can stop the process of communication at early stage.

**Attack:** Distance Fraud Attack

**Description:** A malicious node can come closer to subgroup and make false claim to be the nearest node. [7, 38, 39]. Let $EVENT^i_{SG^{HL_a}_{SC_e}}$ and $EVENT^i_{SG^{HL_a}_{SC_d}}$ are the events when $SG^{HL_a}_{SC_e}$ and $SG^{HL_a}_{SC_d}$ find collision. A collision can occur when some bits are not verified. Now, success probability of distance fraud attack can be calculated as:

$$\begin{aligned} & P[EVENT^i_{SG^{HL_a}_{SC_e}} \cap EVENT^i_{SG^{HL_a}_{SC_d}}] \\ = \; & (P[EVENT^1_{SG^{HL_a}_{SC_e}}]P[\frac{EVENT^2_{SG^{HL_a}_{SC_e}}}{EVENT^1_{SG^{HL_a}_{SC_e}}}] \\ & \cdots P[\frac{EVENT^n_{SG^{HL_a}_{SC_e}}}{\Pi_{i=1}^{n-1} EVENT^i_{SG^{HL_a}_{SC_e}}}]_{HEH=satisfactory} \\ & +(P[EVENT^1_{SG^{HL_a}_{SC_d}}]P[\frac{EVENT^2_{SG^{HL_a}_{SC_d}}}{EVENT^1_{SG^{HL_a}_{SC_d}}}] \\ & \cdots P[\frac{EVENT^n_{SG^{HL_a}_{SC_d}}}{\Pi_{i=1}^{n-1} EVENT^i_{SG^{HL_a}_{SC_d}}}]_{HEH=satisfactory}. \end{aligned}$$

Now, when $DIR^1_{SG^{HL_a}_{SC_d}}$ or $DIR^1_{SG^{HL_a}_{SC_e}}$ is zero then:

$$\begin{aligned} & P[EVENT^i_{SG^{HL_a}_{SC_e}} \cap DIR^i_{SG^{HL_a}_{SC_e}} \\ & \qquad \cap HEH\_AND^{MN_a}_{SG^{HL_a}_{SC_d}} = satisfactory] \\ = \; & \frac{1}{2}(\frac{1}{p_{90}}+\frac{1}{p_{80}}+\frac{1}{p_{70}}+\frac{1}{p_{60}}+\frac{1}{p_{50}}) \\ = \; & P[EVENT^i_{SG^{HL_a}_{SC_d}} \cap DIR^i_{SG^{HL_a}_{SC_d}} \\ & \qquad \cap HEH\_AND^{MN_a}_{SG^{HL_a}_{SC_d}} = satisfactory]. \end{aligned} \tag{6}$$

When $DIR^1_{SG^{HL_a}_{SC_d}}$ or $DIR^1_{SG^{HL_a}_{SC_e}}$ is one then:

$$\begin{aligned}
& P[EVENT^i_{SG^{HL_a}_{SC_e}} \cap DIR^1_{SG^{HL_a}_{SC_e}} \\
& \quad \cap HEH_AND^{MN_a}_{SG^{HL_a}_{SC_e}} = satisfactory] \\
= \; & P[EVENT^i_{SG^{HL_a}_{SC_e}} \cap DIR^i_{SG^{HL_a}_{SC_e}}] \\
& \quad P[HEH_AND^{MN_a}_{SG^{HL_a}_{SC_e}} = satisfactory] \\
= \; & P[(EVENT^i_{SG^{HL_a}_{SC_e}} \\
& \cap VER^{CHA^1} = h[K, N_{SG^{HL_a}_{SC_d}}, N_{SG^{HL_a}_{SC_e}})] \\
& P[DIR^i_{SG^{HL_a}_{SC_e}}]P[HEH_AND^{MN_a}_{SG^{HL_a}_{SC_e}} = satisfactory] \\
& + P[(EVENT^i_{SG^{HL_a}_{SC_e}} \\
& \cap VER^{CHA^1} \neq h[K, N_{SG^{HL_a}_{SC_d}}, N_{SG^{HL_a}_{SC_e}})] \\
& P[DIR^i_{SG^{HL_a}_{SC_e}}]P[HEH_AND^{MN_a}_{SG^{HL_a}_{SC_e}} = satisfactory] \\
= \; & (\frac{3}{4})^i + (\sum_{i=1}^{n}(\frac{1}{p_{i-1}})^{n-i-2} * (\frac{1}{p_{protected}})^{n-i-2} \\
& + (\frac{1}{p_{90}} + \frac{1}{p_{80}} + \frac{1}{p_{70}} + \frac{1}{p_{60}} + \frac{1}{p_{50}})^{n-i-2}). \qquad (7)
\end{aligned}$$

Since collision is found in one of the two sides thus in this case also probability is considered to be $\frac{1}{2}$. Equation (7) gives the value of acceptance rate of attack. Higher value of trust reduces the chances of this attack to a great extent.

**Attack:** Terrorist Fraud Attack.

**Description:**In this attack, existing $M^{(a,b)}_{(c,d)}$ act as malicious entity. $M^{(a,b)}_{(c,d)}$ collaborate with $MM^{(a,b)}_{(c,d)}$ and tries to convince $MSG^{HL_a}_{M^{(a,b)}_{(c,d)}}$ that he is nearby when he is not [7, 39, 38]. This attack can be protected using secret sharing scheme [8]. $P$[success of terrorist fraud attack] $\geq$ $P$ [success of mafia fraud attack]. Let $P[M^{(a,b)}_{(c,d)} \rightarrow MM^{(a,b)}_{(c,d)} : Cert(MN^{HL_i}_{SM_{j+1}}), N_M, SKAL_M] = \frac{1}{pterrorist}$. $P[MM^{(a,b)}_{(c,d)} \rightarrow M^{(a,b)}_{(c,d)} : Cert(VN^{(a,b)}_{(c,d)})]_{HEH\_AND^{MN_a}_{M^{(a,b)}_{(c,d)}}} = \frac{1}{p_{terrorist}} + \frac{1}{p_{90}} + \frac{1}{p_{80}} + \frac{1}{p_{70}} + \frac{1}{p_{60}} + \frac{1}{p_{50}}$. Since symmetric key $K$ is known to all thus $P[M^{(a,b)}_{(c+1,d)} \rightarrow MM^{(a,b)}_{(c,d)} : E_{PK_{VN^{(a,b)}_{(c,d)}}}\{SK_{M^{(a,b)}_{(c+1,d)}}\}]_{HEH\_AND^{MN_a}_{M^{(a,b)}_{(c,d)}}} = (\frac{1}{p_{terrorist}} + \frac{1}{p_{90}} + \frac{1}{p_{80}} + \frac{1}{p_{70}} + \frac{1}{p_{60}} + \frac{1}{p_{50}})^2$. and it is easy to mislead any communication by existing members. With increase in such communication chances of terrorist fraud detection increases because trust score decreases. If probability of $M^{(a,b)}_{(c,d)}$ for self answered question is marked as $\frac{1}{p_{self\_answered}}$ then $P$[success of terrorist fraud attack]=$(\frac{1}{p_{self\_answered}})^q * (\frac{1}{p_{terrorist}} + \frac{1}{p_{90}} + \frac{1}{p_{80}} + \frac{1}{p_{70}} + \frac{1}{p_{60}} + \frac{1}{p_{50}} + (t-1)/t + p_{self\_answered})^q$. where '$t$' is the total number of queries exchanged between $M^{(a,b)}_{(c,d)}$ and $MM^{(a,b)}_{(c,d)}$ and collision does not found in $q$ rounds.

**Attack:** Distance Hijacking Attack

**Description:** This attack is different from distance fraud and terrorist fraud attack. In distance fraud, a dishonest prover and verifier are involved. In terrorist fraud, dishonest prover involves with other attacker but in the distance hijacking attack, dishonest prover interacts with honest prover and involves them for false distance [21]. In distance hijacking attack, minimum single dishonest prover is involved with the other honest parties. If other parties behave like dishonest prover or verifiers then this attack become distance fraud attack. Now, $P$[Success of distance hijacking attack] $\leq$ $P$[Success of distance fraud attack] [38]. $P$[Success of distance hijacking attack] = $P$ [honest nodes reveal secret information without being dishonest]. Any dishonest node can behave as honest through masquerading, impersonation, taking false ownership, etc. This dishonest behavior in tags can be checked through birthday paradox and trust score. Now according to birthday paradox, probability of matching two numbers when number of nodes are 10 in each subgroup is less than $\frac{1}{8}$. Further, trust score reduces the probability of this attack to $(\frac{1}{p_{90}} + \frac{1}{p_{80}} + \frac{1}{p_{70}} + \frac{1}{p_{60}} + \frac{1}{p_{50}})$. This probability of success of distance hijacking attack due to trust score is much less than $\frac{1}{8}$.

## 4.2 Performance Analysis

In this section, network performance is analyzed using various QoS parameters: delivery ratio, goodput, coverage, energy consumption and jitter. This analysis is performed using 150-nodes scenarios on ns-3 simulator. In order to construct MANET, a smart node is formed by integrating RFID reader with mobile sensor node. These mobile smart nodes constitute a hierarchical Ad-hoc network as shown in Figure 2. Reader collects the data from its local network and transmits to other nodes through radio frequency antenna of sensor nodes. Performance analysis of QoS parameters is as follows.

**Delivery Ratio.** It is the ratio of number of sent packets to number of delivered packets toward sink. Figure 4 shows the delivery ratios of 150 nodes over five MANETs routing protocols: Ad-hoc On Demand Distance Vector (AODV), Destination Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR), Temporarily Ordered Routing Algorithm (TORA) and Zone Routing Protocol (ZRP). From both scenarios, it is observed that ZRP protocol outperforms the other routing protocols. In 150 nodes scenarios, delivery ratio decreases with increase in time for every protocol because the number of available nodes for data transmission decreases and more number of nodes are occupied for routing.

**Goodput.** Another non-overlapping term with delivery ratio is goodput. It is the total number of successfully delivered packets to sink [54]. With addition of more number of packets and delay parameters, value of goodput can be increased. Figure 5 and Figure 6

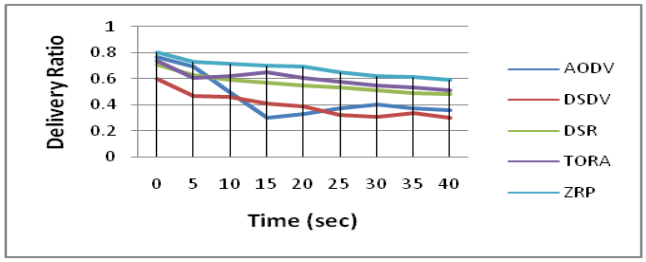


Figure 4: Delivery ratio for 150 nodes over MANETs routing protocols

Table 4: Lightweight node-packet delivery analysis using alloy (time in msec)

| Percentage of routed or delivered packets | Intruder Assertions | Proposed Trusted Strategy | |
|---|---|---|---|
| | | Time (Steps) | Result |
| More than 75 | 1/5/10 | 10/21/32 (80/113/131) | Proved |
| More than 65 | 1/5/10 | 60/94/145 (150/173/224) | Proved |
| More than 55 | 1/5/10 | 113/146/211 (170/210/563) | Proved |

show the goodput for 150 nodes at offer load of 1 packet/second and 5 packets/second respectively. In 150-nodes scenarios, ZRP protocol outperforms than any other protocol. Performance of ZRP protocol is average and it is increasing exponentially with time at lesser rate, i.e. 1 pkt/sec.. In 5pkt/sec. for 150 nodes, ZRP is having improved performance as compared to 1 pkt/sec. In these scenarios, other protocols also show increase in performance but this increase is lesser as compared to ZRP protocol. It is also observed that in 150 nodes scenarios, growth of throughput for ZRP is linear than linear but for other protocol, it is linear or less.

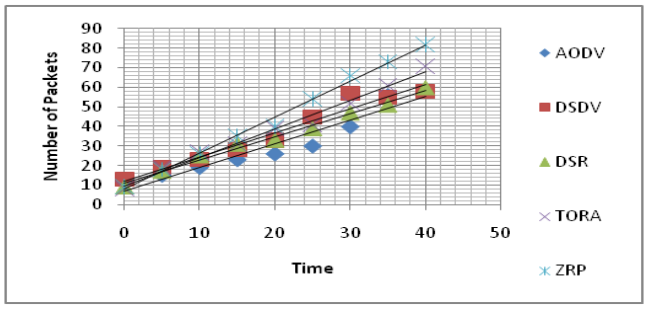


Figure 5: Goodput for 150 nodes at 1 packet/second

**Coverage.** It is defined as number of nodes used per unit time for successful transmission of packets. In Table 4, three scenarios are taken into consideration to find the coverage range for proposed scheme. Results shows that if a node deliver more than 75% of packets then intrusion detection take 50 msec and 70 steps which is lesser than delivery percentage of 65. It takes a minimum difference of 100 msec. and 90 steps when compared with 55% of delivery. Hence, a node is considered to be covered if it successfully delivers 75% of packets it receive and loss 25% only for performance analysis. Figure 7 and Figure 8 show the coverage of 150 nodes at 1pkt/sec and 5 pkts/sec respectively. In 1pkt/sec and 5 pkts/sec. scenarios, DSR and TORA are having worst performance variance. In both such scenarios, ZRP outperforms the other protocols because of its hybrid routing nature. This protocol, internally divides the nodes into zone and these zones with energy saving Frisbee formation save nodes energy for communication. Most of the nodes are silent during simulation initialization and this property is common among all scenarios. High coverage is observed during peak hours which varies from protocol to protocol.

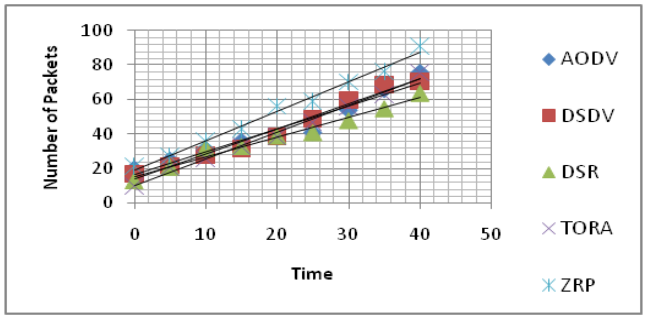


Figure 6: Goodput for 150 nodes at 5 packets/second

**Energy Consumption.** The evaluation of energy consumption in simulation environment is observed through throughput. Whenever radio of any node is on and a byte is transferred then energy of node is considered to be consumed. As discussed in section 4, this energy is calculated from RSSI and it is a function of distance. More is the distance parameter more will be the energy consumption. Figure 9 shows the average energy consumption for 150 nodes scenario. If bursts of any protocol are closer to the outer ring then average energy consumption for that protocol is higher and it is called as high burst (0.04-0.05 Joules). Low bursts are the minimum consumption values that are close to origin (0.01 Joules). Whereas, medium bursts are the intermediate values between high and low bursts (0.02-0.03 Joules). As shown in Figure 9, ZRP and TORA protocol are having higher average energy consumption than AODV, DSDV and DSR for o.1 pkt/sec, 1 pkt/sec. and 5 pkts/sec. In DSR and DSDV protocol, energy consumption shows

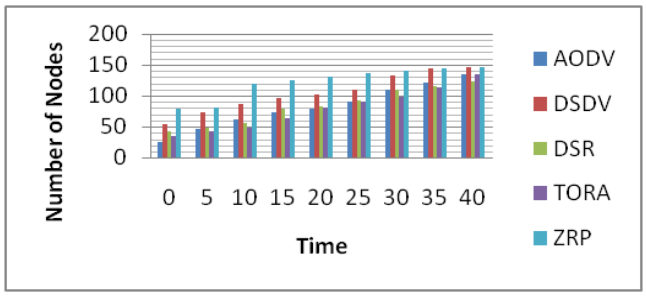


Figure 7: Coverage for 150 nodes at 1 packets/second

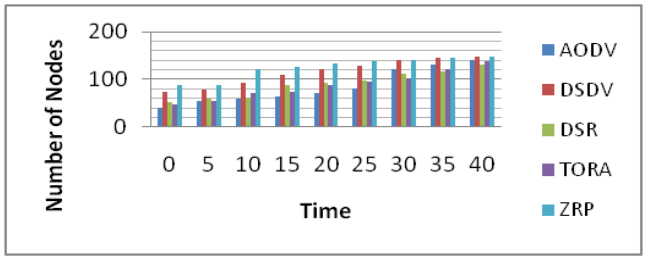


Figure 8: Coverage for 150 nodes at 5 packets/second

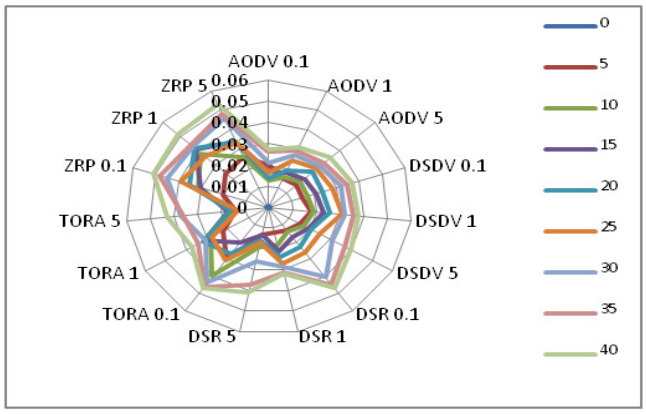


Figure 9: Energy consumption for 150 nodes during simulation time

variations with increases in packet/second. because of dynamic nature of routing protocol. Whenever there is need to transmit packets, then only nodes are activated and energy consumption starts.

**Jitter.** It is an average value of root mean square delay. Figure 10 shows the jitter values at different packet delivery rates, i.e. 1 pkt/sec. and 5 pkts/sec. Jitter values of TORA and AODV are worst as compared to other protocols. Since ZRP provides higher throughput but at minimum jitter thus it is considered to be the best protocol. Jitter value decreases with increase in number of nodes because more nodes are available to route the packets thus delay decreases. But this delay does not affect much on the performance because the packet delivery rate also increases. Performance improvement because of increased number of nodes is compensated by increase in packet delivery ratio. Also, with increase in packet delivery ratio the jitter decreases because once routes are established then it does not affect much on the performance.

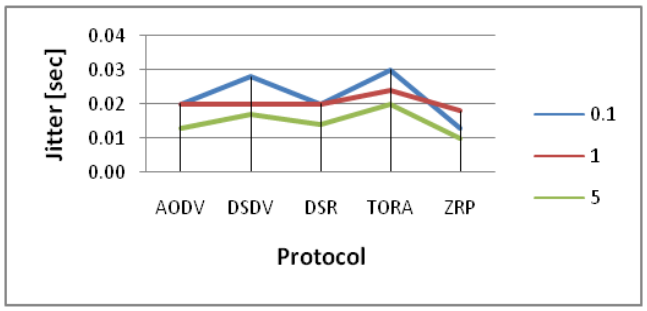


Figure 10: Jitter for 150 nodes at different delivery rate

## 4.3 Lightweight Analysis

### 4.3.1 Lightweight Primitive Analysis

Confidentiality as well as authentication mechanisms are integrated with protocol 1 and protocol 3 whereas only authentication mechanism is integrated with protocol 2. Table 5 shows the comparative analysis of substitution permutation network (SPN) based lightweight primitives for Protocols 1, 2 and 3. Two lightweight primitives are taken for analysis: LED and PHOTON. Result of lightweight primitives are compared with classical mechanism, i.e. Advanced Encryption Standard (AES). All three are based on confusion and diffusion layer principle in SPNs. LED and AES are used to achieve confidentiality and PHOTON is used for authentication. Alloy analysis shows that the number of variable generated, clauses formed and computational time in Protocol 1 and Protocol 3 for LED and PHOTON are much lesser than AES. Both confusion and diffusion layers are showing similar results. Multiple challenges and verifications in Protocol 2 increases the resource consumption and time required to complete the operations. Comparison of lightweight primitives with classical primitive shows that integration of LED and PHOTON in proposed mechanism enhances the performance of protocols as compared to AES based classical confidentiality mechanism.

### 4.3.2 Lightweight Policy Analysis

Figure 11 shows the proposed trust policy for subgroup member in proposed scheme. Trust based proposed mechanism is having: subgroup controller, subgroup member, virtual subgroup member and virtual subgroup controller. Each entity in hierarchical model acts as either producer or consumer. While acting as producer or consumer, there will be change of permissions. A subgroup controller will be having READ, WRITE, ACCESS, USE, MODIFY permissions for trust management. Whereas, a subgroup

Table 5: Simple vs. lightweight primitive analysis for proposed scheme

| Protocol | Primitives | Layer | Variables | Clauses | Time(msec) |
|---|---|---|---|---|---|
| Protocol1 | LED | Confusion | 22025 | 15174 | 1463 |
| | | Diffusion | 20451 | 13012 | 1231 |
| | PHOTON | Confusion | 42314 | 44101 | 2112 |
| | | Diffusion | 36110 | 23603 | 1642 |
| | AES | Confusion | 80178 | 25545 | 3463 |
| | | Diffusion | 60145 | 160234 | 2654 |
| Protocol2 | PHOTON | Confusion | 44114 | 46045 | 2414 |
| | | Diffusion | 37111 | 26032 | 2001 |
| Protocol3 | LED | Confusion | 22544 | 160112 | 1513 |
| | | Diffusion | 20653 | 13009 | 1213 |
| | PHOTON | Confusion | 41015 | 44023 | 2104 |
| | | Diffusion | 36009 | 23112 | 1672 |
| | AES | Confusion | 81534 | 26123 | 3413 |
| | | Diffusion | 62435 | 16144 | 2611 |

```
(MemberAssigned = (Interested s a r):- (Assigned s r) (AssignID a) (SubGroup r))
(MemberConflict = (Interested s a r):- (Conflicted s r) (RetrieveID a) (SubGroup r))
(MemberTrust = (TrustGeneration s a r):- (Assigned s r) (AssignID a) (SubGroup r))
(MemberTrust = (TrustPropagation s a r):- (Assigned s r) (AssignID a) (SubGroup r))
(MemberTrustConflict = (TrustAccumulation s a r):- (Conflicted s r) (SubGroup r))
(MemberTrust = (TrustPrediction s a r):- (Assigned s r) (AssignID a) (SubGroup r))
(MemberTrustConflict = (TrustEvaluate s a r):- (Conflicted s r) (SubGroup r))
(MemberTrustConflict = (TrustApplication s a r):- (Conflicted s r) (SubGroup r))
```

Figure 11: Margrave policy for access control in proposed scheme

member will be having READ, ACCESS, USE permissions only. So, each member will have its own policy in the network. Figure 11 shows the subgroup member policy for TrustGeneration, TrustPropagation, TrustAccumulation, TrustPrediction, TrustEvaluation and TrustApplication. A subgroup member can act as producer to assign new identification to new node or retrieve its identification. Trust generation, propagation and prediction are permissible for subgroup member. Trust accumulation and application comparison are not allowed for member but these are considered to be the functions of subgroup controller. After designing and analyzing the policies of every member in proposed scheme, it is analyzed through Margrave that there is no conflict in any policy [1].

# 5 Conclusions

The current study examines RFID-Sensor based MANETs using ECCr in code based cryptography. MANETs are constructed by extending the trust management approach in resource constraint environment with Teo and Tan protocol for key exchange using hierarchical model [66] and Avoine MA-KA2 protocol for distance bounding and mutual authentication [7]. These approaches are perceived as efficient lightweight approaches with strong protection against distance bounding attacks. QoS parameters taken for network performance analysis are: delivery ratio, goodput, coverage, energy consumption and jitter. In conclusion, 150 nodes scenario shows that ZRP protocol outperforms any other protocol for proposed security system using trust management. Maximum goodput that is achievable through best routing protocol is approximately 80 packets per second to minimum delay of 0.03 msec. Probability attack analysis is performed for mafia fraud attack, distance fraud attack, terrorist fraud attack and distance hijacking attack in distance bounding protocol. In this analysis, fault acceptance rate of system is checked and in result it is found that system is strong enough against all these attacks. Lightweight primitives and policies for subgroup members are also analyzed. It is found that integration of lightweight primitives reduce computation and time complexity. Lightweight policy analysis shows that there is no conflict in access domains of any subgroup member.

## References


[1] *The Margrave Policy Analyzer*, Jan. 19, 2015. (http://www.margrave-tool.org)

[2] M. R. S. Abyaneh, *Security Analysis of Lightweight Schemes for RFID Systems*, PhD thesis, University of Bergen, Norway, 2012.

[3] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, "Scalable RFID systems: A privacy-preversing proto with constant-time identification," *IEEE Transactions on Parallel Distribution Systems*, vol. 23, no. 8, pp. 1536–1550, 2012.

[4] R. J. Anderson, *Security Engineering: A guide to Building Dependable Distributed Systems*, New York, USA, John Wiley & Sons, 2001.

[5] S. A. Anson and M. Ilyas, *RFID handbook: Application, technology, security and privacy*, Boca Raton, Florida, USA, CRC, 2008.

[6] P. D'Arco and A. De Santis, "On ultralightweight RFID authentication protocols," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 4, pp. 548–563, 2011.

[7] G. Avoine and C. H. Kimh, "Improving program analyses by structure untupling," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 830–839, 2013.

[8] G. Avoine, C. Lauradoux, and B. Martin, "How secret-sharing can defeat terrorist fraud," in *Proceedings of the 4th ACM Conference on Wireless Network Security*, pp. 145–155, Hamburg, Germany, June 15-17, 2011.

[9] N. Bagheri and M. Safkhani, "Secret disclosure attack on kazahaya, a yoking-proof for low-cost RFID tags," Technical Report Cryptology ePrint Archive: Report 2013/453, July 2013.

[10] J. D. Bakos, D. M. Chiarulli, and S. P. Levitan, "Lightweight error correction coding for system-level interconnects," *IEEE Transactions on Computing*, vol. 56, no. 3, pp. 289–304, 2007.

[11] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*, Springer-Verlag Berlin Heidelberg, New York, USA, Springer, 2009.

[12] M. Burmester, T. V. Le, and B. D. Medeirosn, "Universally composable RFID identification and authentication protocols," *ACM Transaction on Information and Systems Security*, vol. 12, no. 4, pp. 21:1–21:33, 2012.

[13] M. Burmester and J. Munilla, "Lightweight RFID authentication with forward and backward security," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 11:1–11:26, 2011.

[14] A. Canteaut and F. Chabaud, "Improvement of the attacks on cryptosystems based on error-correcting codes," Research Report: LIENS-95-21, École Normale Supérieure, Paris, July 1995.

[15] T. Cao, E. Bertino, and H. Lei, "Security analysis of the sasi protocol," *IEEE Transactions on Dependable and Secure Computing*, vol. 6, no. 1, pp. 73–77, 2009.

[16] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao, "Habitat monitoring application driver for wireless communication technology," in *Proceedings of the ACM SIGCOMM Workshop on Data Communication in Latin America and the Caribean*, pp. 20–41, San Jose, Costa Rica, Apr. 2001.

[17] A. Chakrabarti, A. Sabharwal, and B. Aazhang, "Using predictable observer mobility for power efficient design of sensor networks," in *Proceedings of the 2nd International Workshop on Information Processing in Sensor Networks (IPSN-03)*, pp. 129–145, Palo Alto, CA, USA, Apr. 2003.

[18] R. Chen, X. Chao, L. Tang, J. Hu, and Z. Chen, "A global reputation-based trust model in peer-to-peer networks," in *4th International Conference Automatic and Trusted Computing (ATC 2007)*, pp. 203–215, Hong Kong, China, 2007.

[19] J. Cho, Y. Shim, T. Kwon, and Y. Choi, "Sarif: A novel framework for integrating wireless sensor and RFID networks," *IEEE Wireless Communications*, vol. 14, no. 6, pp. 50–56, Dec. 2007.

[20] M. Conrad, T. French, and W. Huang, "A lightweight model of trust propagation in a multi-client network environment. to what extent does experience matter?," in *International Conference on Avaiability, Reliability and Security (ARES'06)*, pp. 482–487, Vienna University of Technology, Austria, Apr. 20-22, 2006.

[21] C. Cremers, K. B. Rasmussen, B. Schmidt, and S. Capkun, "Distance hijacking attacks on distance bounding protocols," in *IEEE Symposium on Security and Privacy (SP'12)*, pp. 113 – 127, San Francisco, CA, USA, 20-23 May 2012.

[22] D. Denning, "A new paradigm for trusted systems," in *Proceedings on the 1992-1993 Workshop on New Security Paradigms*, pp. 36–41, New York, NY, USA, 1993.

[23] M. Deutch, "Cooperation and trust: Some theoretical notes," in *Nebraska Symposium on Motivation*, pp. 275–319, University of Nebraska Press, Lincoln NE, USA, 1962.

[24] C. Englund and H. Wallin, "RFID in wireless sensor network," Master Thesis, Communication Systems Group, Department of Signals and Systems, Chalmers University of Technology, Goteborg, Sweden.

[25] A. Ephremides, "Energy concerns in wireless networks," *IEEE Transactions on Wireless Communication*, vol. 9, no. 4, pp. 48–59, 2002.

[26] R. B. Ferguson, "Gentag patent adds RFID sensor network feature to mobile devices," Dec. 2006. (`http://www.eweek.com/c/a/Mobile-and-Wireless/Gentag-Patent-Adds-RFID-Sensor-Network\-Feature-to-Mobile-Devices\`)

[27] M. D. Francesco, S. K. Das, and G. Anastasi, "Data collection in wireless sensor networks with mobile elements: A survey," *ACM Transaction on Sensor Networks*, vol. 8, no. 1, pp. 7:1–7:31, 2011.

[28] D. Gambetta, "Can we trust?," in *Trust: Making and Breaking Cooperative Relations*, vol. 13, pp. 213–237, Department of Sociology, University of Oxford, England, 2000.

[29] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 2, pp. 279–298, 2012.

[30] D. Jackson, "Alloy: a lightweight object modelling notation," *ACM Transactions on Software Engineering and Methodology*, vol. 11, no. 2, pp. 256–290, 2002.

[31] D. Jackson, "Micromodels of software: Lightweight modelling and analysis with alloy," Technical Report MIT Lab Manual, Feb. 2002.

[32] S. Jarvenpaa, K. Knoll, and E. L. Dorothy, "Is anybody out there?: antecedents of trust in global virtual teams," *Journal of Management*, vol. 14, no. 4, pp. 29–64, 1998.

[33] A. Josang, "The right type of trust for distributed systems," in *Proceedings of the ACM New Security Paradigm Workshop*, pp. 119–131, Lake Arrowhead, CA, USA, 1996.

[34] A. Juel and S. Weis, "Authenticating pervasive devices with human protocols," in *Advances in cryptology (Crypto'05)*, pp. 293–298, Santa Barbara, California, USA, 2005.

[35] A. Juels, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communication*, vol. 24, no. 2, pp. 381–394, 2005.

[36] S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the International World Wide Web Conference (WWW'03)*, pp. 640–651, Budapest, Hungary, 2003.

[37] O. Khalid, U. S. Khan, S. A. Madani, et al., "Comparative study of trust and reputation systems for wireless sensor networks," *International Journal on Security and Communication networks*, vol. 6, no. 6, pp. 669–688, 2013.

[38] C. H. Kim, "Security analysis of ykhl distance bounding protocol with adjustable false acceptance ratio," *IEEE Communications Letters*, vol. 15, no. 10, pp. 1078–1080, 2011.

[39] C. H. Kim and G. Avoine, "RFID distance bounding protocols with mixed challenges," *IEEE Transactions on Wireless Communications*, vol. 10, no. 5, pp. 1618–1626, 2011.

[40] P. Kitsos and Y. Zhang, *RFID security, techniques, protocols and system-on-chip design*, New York, USA, Springer, 2008.

[41] R. Koh, E. Schuster, I. Chackrabarti, and A. Bellman, "Securing the pharmaceutical supply chain," White Paper, 2003.

[42] A. Kumar and A. Aggarwal, "Efficient hierarchical threshold symmetric group key management protocol for mobile ad hoc networks," in *International Conference on Contemporary Computing (IC3'12)*, pp. 335–346, Noida, India, 2012.

[43] A. Kumar, K. Gopal, and A. Aggarwal, "Outlier detection and treatment for lightweight mobile ad hoc networks," in *Qshine'13*, pp. 750–763, Greater Noida, India, 2013.

[44] M. Lehtonem, T. Staake, F. Michahelles, and E. Fleisch, "From identification to authentication- a review of RFID product authentication techniues," in *Networked RFID Systems and Lightweight Cryptography*, pp. 169–187, USA, 2007.

[45] A. Mason, A. Shaw, A. I. Al-Shamma'a, and T. Welsby, "RFID and wireless sensor integration for intelligent tracking systems," in *Proceedings of 2nd GERI Annual Research Symposium (GARS'06)*, Liverpool, U.K., 2006.

[46] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of Management Executive*, vol. 20, no. 3, pp. 709–734, 1995.

[47] A. McCumber, *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*, Boca Raton, Florida, USA, Auerbach Publications, 2005.

[48] D. H. McKnight and N. L. Chervany, "Trust and distrust definitions: One bite at a time," in *Deception, Fraud, and Trust in Agent Societies*, pp. 27–54, Barcelona, Spain, 2000.

[49] G. E. Moore, "Cramming more components onto integrated circuits," *Electronics Magazine*, vol. 38, no. 8, pp. 114–117, 1965.

[50] Z. Nochta, T. Staake, and E. Fleisch, "Product specific security features based on RFID technology," in *International Symposium on Applications and the Internet Workshops (SAINTW'06)*, pp. 72–75, Phoenix, AZ, USA, 2006.

[51] D. M. R. Overbeck, *Public Key Cryptography based on Coding Theory*, Ph.D. Thesis, Technische Universitat Darmstadt, 64277 Darmstadt, 2007.

[52] J. Pearson, "Securing the pharmaceutical supply chain with RFID and public key infrastructure (PKI) technologies," White Paper, June 2005.

[53] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Esteveze-Tapiador, and A. Ribagorda, "RFID systems: A survey on security threats and proposed solutions," in *International Conference on Personal Wireless Communication (PWCA'06)*, pp. 159–170, Albacete, Spain, 2006.

[54] D. Puccinelli and M. Haenggi, "Reliable data delivery in large scale low-power sensor networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 4, pp. 28:1–28:41, 2010.

[55] V. Rajendran, J. J. Garcia-Luna-Aceves, and K. Obraczka, "Energy-efficient, application-aware medium access for wireless sensor networks," in *Proceedings of the 2005 International Conference on Mobile Ad Hoc and Sensor Systems Conference (MASS'05)*, pp. 623–630, Washington, DC, USA, 2005.

[56] V. Rajendran, K. Obraczka, and J. J. Garcia-Luna-Aceves, "Energy-efficient, collision free medium ac-

cess control for wireless sensor networks," *Wireless Networks*, vol. 12, no. 1, pp. 63–78, 2006.

[57] C. Schurgers, V. Tsiatsis, S. Ganeriwal, and M. B. Srivastava, "Optimizing sensor networks in the energy-latency-density design space," *IEEE Transactions on Mobile Computing*, vol. 1, no. 1, pp. 70–80, 2002.

[58] P. W. Shor, "Algorithm for quantum computation: Discrete logarithms and factoring," in *35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, Santa Fe, New Mexico, USA, 1994.

[59] K. Sohrabi, J. Gao, V. Ailawadhi, and G. J. Pottie, "Protocols for self-organization of a wireless sensor networks," *ACM Computer Communication Review*, vol. 7, no. 5, pp. 16–27, 2000.

[60] A. W. Stephen, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *First International Conference on Security in Pervasive Computing*, pp. 201–212, Boppard, Germany, 2003.

[61] H. M. Sun, W. C. Ting, and K. H. Wang, "On the security of chien's ultralightweight RFID authentication protocol," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 2, pp. 315–317, 2011.

[62] Y. Sun, S. Du, O. Gurewitz, and D. B. Johnson, "Dw-mac: A low latency energy efficient demand wakeup mac protocol for wireless sensor networks," in *proceedings of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'08)*, pp. 53–62, New York, USA, 2008.

[63] Y. Sun, W. Yu, Z. Han, and K. J. Ray Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal of Select Area on Communications*, vol. 24, no. 2, pp. 305–317, 2006.

[64] P. Sztompka, *Trust: A sociological theory*, Cambridge, United Kingdom: Cambridge University Press, 1999.

[65] K. Takaragi, M. Usami, R. Imura, R. Itsuki, and T. Satoh, "An ultra small individual recognition security chip," *IEEE Micro*, vol. 21, no. 6, pp. 43–49, 2001.

[66] J. C. M. Teo and C. H. Tan, "Energy-efficient and scalable group key agreement for large ad hoc networks," in *ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN'05)*, pp. 114–121, Montreal, Qc. Canada, 2005.

[67] M. Najam ul islam U. Mujahid and J. Ahmed, "Ultralightweight cryptography for passive RFID systems," Technical Report Cryptology ePrint Archive: Report 2013/847, Dec. 2013.

[68] T. Wu and S. Biswas, "A self-reorganizing slot allocation protocol for multi-cluster sensor networks," in *proceedings of the 4th International Symposium on Information Processing in Sensor Networks*, pp. 309–316, Los Angeles, California, USA, 2005.

[69] R. Yahalom, B. Klein, and Th. Beth, "Trust relationships in secure systems- a distributed authentication perspective," in *Proceedings 1993 IEEE Symposium on Research in Security and Privacy*, pp. 150–164, Oakland, CA, USA, 1993.

[70] X. Yang and N. Vaidya, "A wakeup scheme for sensor networks: Achieving balance between energy saving and end-to-end delay," in *Proceedings of the 10th IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS'04)*, pp. 19–26, King Edward, Toronto, Canada, 2004.

[71] S. Yessad, F. Nait-Abdesselam, T. Taleb, and B. Bensaou, "R-mac: Reservation medimum access control protocol for wireless sensor networks," in *Proceedings of the 32nd IEEE conference on Local computer networks*, pp. 719–724, Dublin, Ireland, 2007.

[72] L. Zhang and Z. Wang, "Integration of RFID into wireless sensor networks: Architectures, opportunities and challenging problems," in *Proceedings of the 5th International Conference on Grid and Cooperative Computing Workshops (GCCW'06)*, pp. 463–469, Changsha, China, 2006.

[73] P. Zhang, C. M. Sadler, S. A. Lyon, and M. Martonosi, "Hardware design experiences in zebranet," in *Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems (SenSys'04)*, pp. 227–238, Baltimore, Maryland, 2004.

[74] Y. Zhang, L. T. Yang, and J. Chen, *RFID and Sensor Networks: Architectures, Protocols, Security and Integrations*, Boca Raton, London, New York: CRC, 2009.

[75] Y. Z. Zhao, C. Miao, M. Ma, J. B. Zhang, and C. Leungi, "A survey and projection on medium access control protocols for wireless sensor networks," *ACM Computing Surveys*, vol. 45, no. 1, pp. 7:1–7:37, 2012.

[76] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.

**Adarsh Kumar** received his ME degree in software engineering from Thapar University, Patiala, Punjab, India, in 2003. Since 2003, he has been with the Department of Computer Science Engineering and Information Technology, Jaypee Institute of Information Technology, Noida, Uttar Pardesh, India, where he is now an assistant professor. His main research interests are cryptography, network security, and adhoc networks.

**Krishna Gopal** biography. received his BTECH degree in electrical engineering from the Department of Electrical Engineering, IIT, Madras, India, in 1966 and his MS and PhD degrees in engineering from the REC Kurukshetra, Kurukshetra, India, in 1972 and 1979, respectively. Since 2011, he has been working asa dean (Academic & Research) with Jaypee Institute of Information Technology, Noida, India. He has forty-five years of teaching and research experience. He is a member of various professional bodies, such as the Life Member System Society of India, the Indian Society for

Technical Education, and the IEEE. .

**Alok Aggarwal** received his BTECH and MTECH degrees in computer science engineering from the Department of Computer science, Kurukshetra University, India, in 1995 and 2001, respectively and his PhD degree in engineering from IIT, Roorkee, India, in 2010. From 2009 to 2012, he worked for the Jaypee Institute of Information Technology, Noida, India. Since 2012, he has been with the JP Institute of Engineering and Technology, Meerut, India, where he is now a professor and director. His main research interests are wired/wireless networks, security, and coding theory.