Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No.2, May 2017 – www.caeaccess.org

Defense Mechanisms in Mobile Ad-hoc Networks

Ola H. Younis
Computer Science & Eng. Dept.,
Faculty of Electronic Eng.,
Menoufia University, Menouf
32952, Egypt

Salah E. Essa
Computer Science & Eng. Dept.,
Faculty of Electronic Eng.,
Menoufia University, Menouf
32952, Egypt

Ayman El-Sayed
Computer Science & Eng. Dept.,
Faculty of Electronic Eng.,
Menoufia University, Menouf
32952, Egypt

ABSTRACT
One of the most important issues for mobile ad-hoc Networks (MANETs) is Security. The feature of MANETs posture both difficulties and openings in accomplishing security objectives, for example, privacy, validation, respectability, accessibility, control of access, and non-repudiation at the end. The techniques of Cryptographic are generally utilized for secure interchanges in wired and remote systems. Most mechanisms of cryptographic, for example, symmetric and asymmetric cryptography, frequently include the utilization of cryptographic keys. Nevertheless, every single cryptographic method will be useless if the management of the key is feeble. The Management of Key is additionally a focal segment in MANET security. The motivation behind key management is to give secure strategies to taking care of cryptographic keying materials.

Keywords
MANET, Defense mechanism, Cryptography, key management, intrusion detection, cooperative enforcement, and trust management.

1. INTRODUCTION
Mobile Ad-Hoc Networks are self-ruling and decentralized remote frameworks. In Mobile Ad-hoc Networks (MANET), every dynamic node goes about as a host and also like a router. The nodes impart to each other by communication of hop-to-hop. [1] The dynamic nature of MANET permits nodes to join and leave the system at any time. Nodes are the frameworks or devices i.e. cell phone, tablet, personal digital assistance, and PC that are partaking in the system and are portable. MANET which using wireless is especially helpless because of its principal qualities, for example, open medium, dynamic topology, appropriated collaboration and obliged ability. Thus, security in MANET is a mind boggling issue.

Key and trust management is a basic supporting component in any security frameworks. Its fundamental operations incorporate building up key swap and amend, and also secret associations. Keys are the essential squares of symmetric and asymmetric cryptographic capacities, which thus outfit confirmation, privacy, uprightness, and non-repudiation security services. The security in systems administration is as a rule subject to appropriate key management. Management of the Key comprises of different administrations, of which each is crucial for the networking system's security.

Trust model: it must be resolved how plenty of different components in the system can believe each other. Subsequently, the trust connections between system components influence the way the key management framework is developed in system.

Trust third party (TTP): [2] a centralized authority (e.g., a key distribution center [KDC] or certification authority [CA]) is trusted by each substance and an element A is trusted by another if the authority claims A is dependable.

Web-of-trust [3]: There is no specific structure exists in such trust charts. Every element deals with its own trust in light of direct suggestion from others.

Localized trust: [4] this model is the center ground of the past two diagrams. A node is trusted if any k trusted substances among the node's one-hop neighbors assert along these lines, inside a limited time period.

Cryptosystems: accessible for the key management, at times just public or symmetric key techniques can be achieved, while in different settings Elliptic Curve Cryptosystems (ECC) are exists. Even though public key cryptography offers more comfort. Public key cryptosystems are somewhat slower than their secret key partners when comparable level of security is required.

There are bunches of trusted models and protocols for routing which are utilized as a part of MANETs to accomplish security. Distinctive trust methods are utilized to give privacy, uprightness and accessibility in mobile ad-hoc network to pick up the safe environment. Supplying trust in MANET is an extra basic errand due to absence of centralized infrastructure. After all, amid the setting out of MANET nodes that are crisp keep returning and matured ones go from the cluster/network, there is interest for keeping up the record additionally to give proper affirmation to the arriving node(s) that are new and in addition the present node(s) in the system. In this paper, A review on different sorts of key management schemes with their unique elements is presented. Additionally, a review of MANET interruption discovery frameworks (IDS), which are responsive ways to deal with upset assaults and utilized as a moment line of protection is also proposed.

In the reset of the paper, a taxonomy of defense mechanisms will be presented in the next section. The discussion of the work and analysis of the future research trend will be proposed in section 3. At the end, the conclusion of the work is revealed in section 4.

2. TAXONOMY OF DEFENSE MECHANISM IN MOBILE AD HOC NETWORKS
Be short of clear networks bounds, shared medium, community oriented services, and mobility nature, all are proposing to a portion of the key qualities that recognize mobile ad hoc networks from the regular ones. Also, every node is a conceivable piece of the basic bolster foundation, coordinate with each other to make fundamental communication services ready. Sending packets or taking an interest in routing process, both of each can specifically influence the security state of the network [5]. The following

is a taxonomy of the defense mechanism as shown in the following figure.

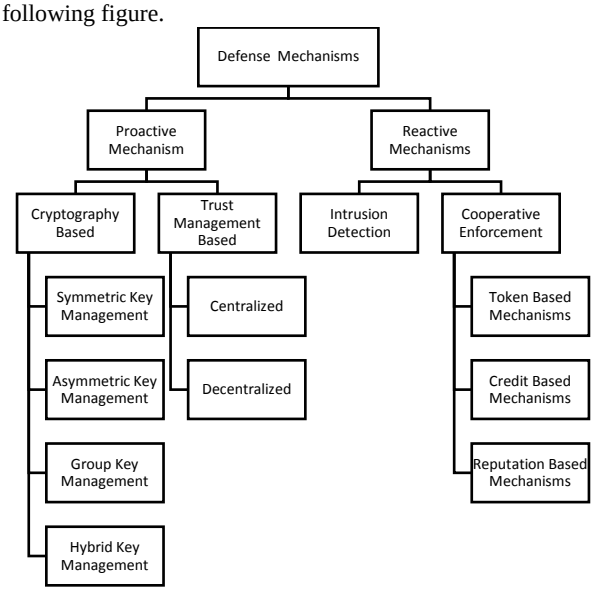

Fig 1: classification of MANET Defense Mechanisms.

2.1 Proactive Mechanism

It comprises of security-mindful routing protocols which avoids event of assaults. These protocols must contemplate the earth components and shape first line of guard as counteractive action is superior to cure. It incorporates trust based system and cryptographic algorithm to guarantee the messages integrity, authentication and confidentiality.

2.1.1 Cryptographic Based Mechanisms

Cryptographic technique [6] is the most widely recognized and solid intends to guarantee security and is not particular to especially ad hoc wireless systems, but rather can be connected to any communication network. This is a portion of the principle methods utilized as a part of MANETs:

Symmetric cryptography: The encryption key is firmly identified with the unscrambling key in that they are indistinguishable as a rule. Practically speaking, keys show a shared secret between at least two gatherings that can be utilized to keep up private communication. Typically the system can pick a common secret key to encode and decode the message once two more gatherings utilize an public/private key match to fabricate confide in the handshake stages, which is more attainable and proficient from a computational angle than asymmetric key methods.

Asymmetric cryptography: It is otherwise called public key cryptography. Out in the public key cryptography, there is a couple of public/private keys. The private key is stored private, although in public key can be public to others. One of the most punctual public key cryptographic strategies, called RSA. Key management, Digital signature, and different procedures have been produced in public-key cryptography, for example, DSA, elliptic curve cryptography, and the ElGamal cryptograph system.

To accomplish the high security in MANET diverse Key Management methods are utilized. Utilizing and overseeing keys for security is an essential errand in MANET because of its energy compelled operations, restricted physical security, variable size of links and dynamic topology. Diverse cryptographic keys are utilized for encryption like public key, symmetric key, group key and hybrid key (symmetric key + asymmetric key). [7]

In symmetric key management alike keys are utilized by sender and recipient. This key is utilized for encryption the information and for decoding the information. In the event that n nodes need to convey in MANET k number of keys are needed, where k = n (n-1)/2.

In Asymmetric key management, two keys are utilized one public key and another private key. Distinctive keys are utilized for encryption and decoding. In every communication, new match of public and private key is made. It needs less number of keys when contrasted with symmetric key cryptography. Asymmetric keys are utilized for short messages however symmetric keys are utilized for long messages if n nodes need to convey in MANET, k number of keys are required, where

$$k = 2n$$

In Group key management, a solitary key which is relegated just for one group of portable nodes in MANET. For setting up a group key, it is making and conveying a secret for group individuals [8]. There are particularly three classifications of group key protocol which are:

centralized, where controlling and rekeying of group is being finished by one element, distributed, group individuals or a portable node which comes in group are similarly in charge of making the group key, circulate the group key and furthermore to rekeying the group, and decentralized, one element and more are in charge of making, disseminating and rekeying the group key.

In Hybrid or composite key management, keys which are consists of the group of two keys or more and it might be symmetric or an asymmetric or the mix of symmetric & asymmetric key.

2.1.1.1 Symmetric Key Management Schemes in MANET

Distributed Key Pre-Distribution Scheme (DKPS): DKPS fundamentally comprise of three vital stages

Distributed Key Selection (DKS): In the main stage, each node takes the random key from the common set by utilizing omission property. Cover Free Family (CFF) idea is utilizing for assessing the prohibition property, to create a CFF in distributed way probabilistic strategy is utilized. This strategy expels the need of TTP (trusted third party) and increase the dynamicity of the MANET.

Secure Shared-key Discovery (SSD): This is second period of DKPS where each node having a common key with another node. Node can't point out that which key in the ring are just the same as which node. The paltry strategy is utilized for SSD. This technique is not giving security but rather simple to assess in light of the fact that eavesdropping can happen in DKS phase.

Key Exclusion Property Testing (KEPT): Last period of DKPS symmetric key management methods is KEPT. Frequency matrix is utilized for present the connection between versatile nodes key and shared keys it utilizing binary values for developing the matrix. KEPT stage test that is all keys of portable nodes satisfying the immunity property of CFF. Components of DKPS are no need of TTP. DKPS

needs less capacity when contrasted with match pair-wise key accession approach. This method is more productive when contrasted with group key accession [9].

Peer Intermediaries for Key Establishment (PIKE): This method utilize the senor nodes to set up the shared key. PKIE is symmetric key concurrence scheme, it utilizing special secret enter in an arrangement of nodes this model is utilizing the idea of arbitrary key pre-dispersion. In MANET, each match of versatile node imparts a typical secret key to no less than at least 1 delegates. Countenance of this model are great security services, and reasonable versatility [10].

Key Infection (INF): This method is straightforward and each versatile node partakes similarly to making the key formation process. INF structure having no need of cooperative exertion since node goes about as a trust segment, this segment propagation their symmetric key. This model having frail security services however INF having depressed storage cost, depressed encryption, and depressed operation. It is having reasonable scalability with the issue recently section of portable node. Great sources proficient survivability in this model with low mediator [11].

2.1.1.2 Asymmetric Key Management Schemes in MANET

Secure Routing Protocol (SRP): it is made with three nodes and an authoritative authority which fill in as merchant in this model. Merchant is the substance which gives the basic certificate to the versatile nodes. Three nodes are characterized as:

Client Node: which are the ordinary user's portable nodes that is needed to be appeared in MANET.

Server Node: The duty of creating the partial testaments and storing the authentications in index structure through which versatile nodes can ask for the certificate of other portable nodes. On this spot Server Node is the piece of certificate authority (CA).

Combiner Node: it acts as the vital undertaking in SRP demonstrate, Combiner Node joins the partial certificate into the substantial certificate.

Ubiquitous and Robust Access Control (URSA): URSA is effective and furnishes dependable accessibility with having the countenance of encoded local communication. It uses effective limit scheme to communicate the certificate (RSA Certificate) marking keys to every portable node. Every versatile node of MANET amends their certificate intermittently. The usefulness of CA is dispersed to every portable node which present in MANET. In the event that any portable node needs to refresh their certificate than, that node ought to be contact to 1-hop neighbors and demand halfway certificate from a gathering of edge k number of portable nodes. This method produces communicate delay, search disappointment, and corrupts the system security. To shield the system from DOS assault and the expose the marking key URSA utilizing obvious and proactive secret sharing techniques [12].

Mobile Certificate Authority (MOCA): The portable nodes which having incredible computational power, physically more secure and on the premise of heterogeneity those versatile nodes utilized as MOCA nodes in this asymmetric key management scheme. At the point when the nodes are similarly prepared than, MOCA nodes are chosen arbitrarily from the MANET. This method is decentralized and the administrations of CA are dispensed to MOCA nodes (subset of versatile nodes). To discover the protected path in the system is the critical errand in MOCA asymmetric key management scheme [13].

Self-Organized Key Management (SOKM): SOKM show utilizing two neighborhood certificate archives one is refreshed and another is non refreshed authentication repository. For computing the best certificate diagram every node keeps up the non-refreshed authentication archives. Each versatile node creates public key certificate to other portable nodes and every portable node go about as their own dominion. The certificate of public key chain is utilizing for doing the key verification handle. SOKM have extraordinary arrangement flexibility and no poverty of boot strapping procedure. Web-of-trust relationship is utilized for declaration way and it is not emphatically associated which is not reasonable for ad hoc network [14].

Secure and Efficient Key Management (SEKM): This is just a single decentralized asymmetric key management scheme (in light of virtual CA confide in model) which gives point by point, safe strategy for communicating, coordination between secret shareholders, and effective that have greater obligation. This method utilized mesh structure for server gathering. This server bunch comprised with all servers which containing the partial framework private key that used to associate the server gathering. To giving certificate services, keep up the association of the group and for share refreshes SEKM utilizing occasional reference points. The cost of keeping up the structure server group is elevation [15].

Partially Distributed Threshold CA Scheme (Z&H): Somewhat Distributed Threshold CA Scheme was found by Zhou, L. what more, Hass, Z. in 1999 is. At the point when the portable ad hoc system is built, this method is utilizing the idea of CA circulation in threshold mold. Security administrations like disconnected confirmation, extraordinary intrusion resistance, and trust administration by CA (certification authority) are given by Z&H asymmetric key management scheme. The key is created by this model are acknowledged without anyone else's self-organized network (MANET) and partial appropriated threshold CA. The survivability of assets effectiveness is poor although it having the adaptability of CRL (Certificate Revocation List), and affirmation [16].

Self-Organized Key Scheme (SOKS): In the self-composed system every portable node goes about as a particular CA. SOKS was uncovered by Hubaux, P and Capkun, S., Buttya, L. in 2003. It has poor adaptability and poor asset productivity however having the disconnected confirmation and constrained intrusion identification security administrations. SOKS having elevation intermediates encryption processes and elevation storage cost [17].

Key Distribution Technique (ID-C): Set of versatile nodes makes or instate the MANET with utilizing the threshold private key generator ID based scheme. The produced key is acknowledged independent from anyone else composed system. Off net verification, trust management and interruption resistances sort security services are given by ID-C asymmetric key administration conspire. Versatility is given through Id Revocation list with awesome resources effectiveness. This scheme possessing medium intermediates, processes, encryption and capacity cost [18].

Identity-Based Key Asymmetric Management Scheme: Without utilizing environment of PKI Secure Identity-Based Key management schemes is presented by Anil Kapil & SnjeevRana. This scheme comprised with four stages. To confirm the client id and producing the comparing private keys it requires trusted key creation Center. RSA method is utilized to build the private-public key combine; every portable node in MANET fetches his long term public and private key match. The secret key as an ace key is picked by key creation center arbitrarily and also distribute its relating public key. Afterward the security investigation of this model, it gives end-to-end credibility and it keeps the system from very strong compel assault, man in a middle assault and from replay assault. Versatile nodes have no compelling reason to creating their public key and to spread the keys in the system [19].

Three Level Key Management Scheme: Secure and extremely Efficient Three Level Key management scheme for MANET is presented by Wan AnXiong, Yao Huan Gong in 2011. To accomplish three level security in MANET, this method uses ID-Based Cryptography with outset secret sharing, Elliptic Curve Cryptography (ECC) and Bilinear Pairing Computation. ECC gives little keys to versatile nodes and high security level. Key creation and key dissemination security administrations with the aversion from enemies' assault are finished by (t, n) outset secret sharing calculation. Blending innovation gives privacy and verification with less computational cost and diminished correspondence overhead [20].

2.1.1.3 Group Key Management Schemes in MANET

Simple and Efficient Group Key Management (SEGK): Bing Wu, Jie Wu, and Yuhong Dong were uncovered the SEGK demonstrate in 2008. Two multicast tree are built in MANET for enhancing the productivity and keeps up it in a parallel design to accomplish the fault tolerance. SEGK demonstrate calls one multicast tree as a blue tree and another multicast tree as a red one. The association of multicast tree is kept up by organizer. Calculation and circulation of intermediates keying materials to all part is does by gathering organizer using underlying tree joins. To do the normal group key each gathering part i.e. versatile node in MANET, partakes in a share of a last regular group key, which is refreshed occasionally. This method displays the twofold multicast tree arrangement and upkeep protocol, which guarantees that it covers all group individuals. In SEGK method, any portable node or group element can join and leave the system. To guarantee the backward and forward security refreshing of group key is done regularly. Two discovery strategies are portrayed in SEGK demonstrate, (a) Tree Links, when the node portability is not noteworthy discovery is done through tree joins. (b) Periodic Flooding of Control Messages, for elevation portability condition this strategy is utilized [8].

2.1.1.4 Hybrid or Composite Key Management Schemes in MANET

Cluster Based Composite Key Management: This model is revealed in [22]. This model takes the idea of disconnected CA, portable agent, various leveled grouping and partial disseminates key administration. Public key of the individuals are kept up by cluster head that diminishes the issue of storage in PKI. Portable gent give node renouncement and PKG aid in MANET. On the premise of current trust esteem and old public key, cluster head's public key is registered. Utilizing the timestamp in key number key restoration process should be possible effectively. Mobile agent process the part of key disavowal prepare and the determination of PKG nodes. It underpins node extendibility out of various leveled grouping. This method spares arrange transmission capacity and storage room.

Zone-Based Key Management Scheme: This method utilizing ZRP (Zone Routing Protocol) and the work of [23,24]. This method is presented by ThairKhdour and Abdullah Aref in 2012, in this method for every versatile node zone is characterized. Some pre-characterized number is designated to every portable node which relies on upon the separation in hops. Symmetric key administration is utilized by portable node just for intra or inside r (zone radius). Without relies on upon grouping versatile node utilizes asymmetric key management between zone security. It gives effective approach to produce the public key without losing the capacity of creating the certificate [25].

2.1.2 TRUST IN MANET

When creating trust relationship among taking an interest nodes it is basic to empower community improvement of program measurements. This thought is essential to communication and system functional designers. [26][27]. A key thought that blueprints the significance of the subject in connection to the security of Mobile Ad-hoc Networks (MANETS) is that trust is constantly required in creating connections when there is instability. This is in accordance with the issue of MANETs where the unexpected conduct is a key concern. A Trust can likewise be characterized as conduct of a group of relationship among things that share in a procedure, where these affiliations are on the premise of the verification made by the earlier interchanges of substances. Trust may take place between these elements, in the occasion the communication happen to be consistent with the procedure a short time later. In another way trust is the measure of confidence with respect to the conduct of extra things (representatives).In MANET trust could be characterized as a level of conviction as per the conduct of nodes (or agent, substances etc).The likelihood estimation of trust fluctuates from 0 to1, where 0 remain for DISTRUST and 1 remain for TRUST [28].

2.1.2.1 Characteristics of Trust in MANETs

Because of wireless medium of MANETs, qualities and the hypothesis, trust must be warily defined [29]. Trust in MANET fundamental element is as per the following:

A choice procedure to check trust toward a substance must be completely spread in light of the fact that the being of a trusted outsider (case a put stock in focal confirmation expert) can't be assumed, Trust must be affirmed in a well adjustable manner without a lot of communication load and calculation, even while catching the complexities of the trust affiliation, A choice support for MANETs must not trust that node(s) are co-agent. In resource-restricted and asset limited situations it is probably going to be across the board above joint effort [28], Trust can't be static. It is changing, Trust is subjective, Trust is not essentially transitive, Actually X trusts Y and Y trusts Z does not suggest that X puts stock in Z, Trust is considered as unbalanced however basically it is not equal, and Trust is setting subordinate. X may put stock in Y in one perspective at the same time, not in other angle.

In MANETs, the vast majority of the node(s) taking an interest in directing ,requires high computational power all

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No.2, May 2017 – www.caeaccess.org

things considered the node with high battery power is viewed as trusted while a node that has low battery control although is not malignant (i.e., legitimate) is doubted.

2.1.2.2 Centralized Versus Decentralized Trust

Brought together trust alludes to the state in which for each extra node in the framework trust qualities are ascertained by an overall trusted in node. All client node(s) of the strategy ask for this trusted node to give them counsel about extra node(s).The state clarified here has two principle suggestions. To begin with, it's sensible to assume that particular client node(s) are probably going to have unique view in regards to a similar target node. Also every client node wards upon the reliability of this node that is single, along these lines rotating it into only one purpose of disappointment. This reality is concealed in decentralized scheme of the trust issue where a node imparts to each client node consequently being the focal point of its own reality. i.e., client node(s) are responsible for figuring their own one of a kind trust values for any objective node they want. This "bottom up" approach is most broadly executed [31] [27].

2.2 Reactive Mechanism

Existent proactive systems can't safeguard against a wide range of assaults so responsive techniques go about as a moment security divider. Security methods are commonly assault situated i.e. dangers are distinguished first and afterward existing specially MANET protocols are upgraded or new security mindful mechanism are intended to ruin those assaults. These techniques act well within the sight of foreseen assaults however crumple under unidentified and unforeseen assaults. It comprises of identifying routing bad conduct with the assistance of intrusion identification framework and participation implementation minimize minded misbehavior of the node

2.2.1 Intrusion Detection System

2.2.1.1 Overview

Their self-arranging nature, open medium and absence of incorporated control make MANETs powerless against an extensive variety of assaults. Encryption, verification and other standard security methods couldn't give full insurance to MANETs. Hence, intrusion detection methods are exceedingly suggested for these systems [33]. It is exceptionally urgent for the security of MANETs to have proactive barrier components that could recognize any abnormalities before they could upset system operations. Customary intrusion discovery frameworks are intended for wired systems and couldn't be straightforwardly connected to their remote reciprocals [34] [35]. The weaknesses of settled intrusion identification frameworks are clear since they require concentrated elements to control the operations of observing, location and revealing. MANETs by nature are conveyed where no settled foundation is required, along these lines making it irrational to anticipate that incorporated frameworks will be viable in such systems.

With the far reaching of mobile ad hoc networks and their applications, it has turned out to be important to adjust to new element security frameworks [36]. Without a brought together centralized authority for directing and observing, every node in the system goes about as a host and a router. This makes MANETs exceedingly helpless to an extensive variety of assaults. These assaults could abuse the helpful conduct of MANETs for their leverage [37]. Compromising a solitary node in the system could risk the security of the entire system.

MANET IDS agent conceptual architecture is described as follow:

The fundamental approach in MANET [39] is that every portable node runs an IDS specialist autonomously. It needs to watch the conduct of neighboring nodes, recognize nearby interruption, coordinate with neighboring nodes, and, if necessary, settle on choices and take activities.

The proposed architecture of the intrusion detection system [38]

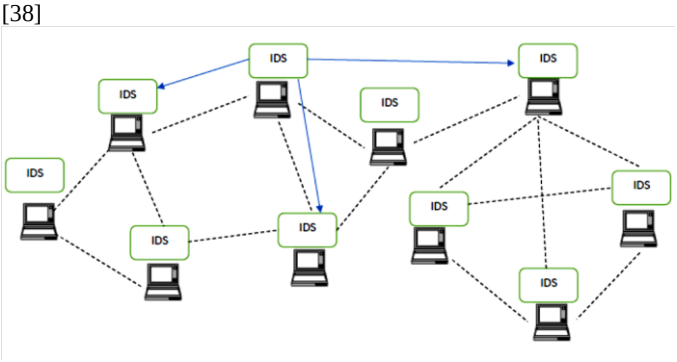

Fig 2: IDS structure

The inward structure of an IDS specialist is appearing in Fig 2.

An IDS operator has information gathering, a local detection engine, neighborhood reaction, a helpful identification engine, worldwide reaction, and secure correspondence with neighboring IDS specialists**.**

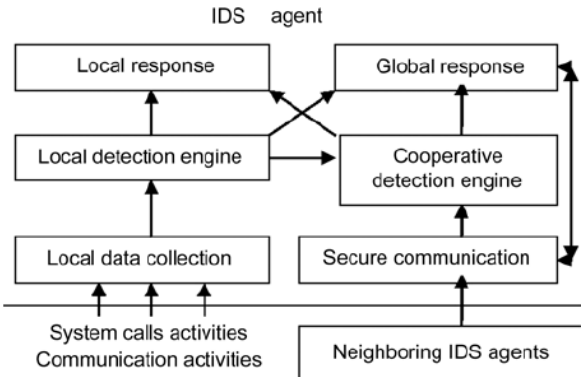

Fig 3: Conceptual model of IDS Agent

In the conceptual model, there are four main functional modules in the IDS agent as show in Fig 3:

Local data collection module [38] this chiefly manages the information collection issue, in which the continuous review information may originate from different assets.

Local detection engine [38] which looks at the local information gathered by the nearby Data accumulation module and investigates if there is any oddity appeared in the information. Since there are constantly new assault sorts rising as the known assaults being perceived by the IDS, the detection engine ought not hope to only perform pattern recognition between known assault behaviors and the peculiarities that are probably going to be a few intrusion: rather than the abuse discovery strategy that can't manage the novel assault sorts viably, the detection engine ought to basically depend on the measurable irregularity recognition strategies, which recognize abnormalities from ordinary behavior in light of the deviation between the present perception information and the typical profiles of the framework.

Cooperative detection engine [38] which works with different IDS agents when there are some needs to discover more confirmations for some suspicious inconsistencies distinguished in some specific nodes. At the point when there is a need to start such collaborated detection process, the members will spread the intrusion identification state data of themselves to the majority of their neighboring nodes, and the majority of the members can compute the new intrusion recognition condition of them in view of all such data they have from their neighbors by some chose algorithm, for example, a disseminated agreement algorithm with weight. Since such a sensible suspicion could be made, to the point that dominant part of the nodes in the impromptu system ought to be generous, it is believed that the conclusion drawn by any of the members that the system is under assault.

Intrusion response module [38] this arrangements with the reaction to the intrusion when it has been affirmed. The reaction can be reinitializing the channel of communication, for example, reassigning the key, or redesigning the network and expelling all the exposed nodes. The reaction to the intrusion behavior shifts with the various types of intrusion.

2.2.1.2 IDS Types

Standalone IDS: Each node contains its own IDS agent, which screen the exercises performed by the node. The node only, if any risk has been identified then it can take security protection locally and because there is no collaboration between nodes then all choices depend on data gathered by nodes. This technique is not all that capable.

Cooperative IDS: Wireless ad hoc network is conveyed in nature so the identification and reaction mechanism must be in two stage. Local and Global discovery. Each node has IDS operator that distinguish assaults locally and coordinates with different nodes inside system and illuminate globally. Altogether, this conveyed agreeable IDS innovation much more steady than independent IDS and steadier level form, cluster based system arrangement. [41] [42].

Hierarchical / Cluster based IDS: Here additionally every node has its own particular IDS operator. Accumulation of nodes cluster form. Each group has an extraordinary node know as cluster head. IDS operator for cluster head is in charge of both local and global Intrusion detection. Layered design in wireless ad-hoc network can be secured by this technique. Another option disseminated arrangement called unconstrained watchdog. Quick sensor ad hoc network without separation them into clusters, some intense autonomous, unconstrained nodes are made, known as watchdog, which screens the contact with their neighbors [43] [44].

Zone based IDS: The local IDS agent utilized as a part of Zone based Intrusion detection system (ZBIDS). Nodes are partitioned into various zones in view of geographical data. Each node has its two ids, INTRA ZONE and INTERZONE and can be defined by Zone ID. By sending HELLO Message, bury and intra zone nodes are resolved. A node might change its job by the way of versatility. [45][46][47]

2.2.1.3 IDS Modes of Operation

An IDS works in view of taking following strategies [48]:

Anomaly based: In peculiarity based IDS typical conduct of system is separated and each movement is checked against it.

Misuse-Based: In this system it can store a mark of intrusion in a database and contrast each time and a progressing action. This IDS works proficiently however falls flat for new assault.

Specification-based: In this IDS, a group of nomination are intended for the network and all progressing exercises are checked against it. Couple of augmentations are likewise accommodated previously mentioned detection frameworks like EAACK-A Secure Intrusion Detection System for MANET [49].It utilizes secure affirmation and misbehavior report confirmation. Computerized signature utilized as a part of this IDS forestalls false affirmation packet.

2.2.1.4 IDS Techniques

Zhang et al. [50]: presented the principal intrusion detection techniques in the versatile ad hoc networks in this presented strategy, a general intrusion recognition structure in MANET was resented, which was conveyed and agreeable to address with the issues of MANET. In this design, each node in the versatile ad hoc networks takes an interest in the intrusion recognition and reaction processes by identifying indications of intrusion conduct locally and autonomously, which are done by the inherent IDS operator. Nonetheless, the neighboring nodes can impart their examination results to each other and coordinate in a more extensive territory. The collaboration between nodes for the most part happens when a specific node recognizes an oddity however does not have enough confirmation to make sense of what sort of intrusion it has a place with. In this circumstance, the node that has distinguished the peculiarity requires different nodes in the correspondence range to perform quests to their security sign with a specific end goal to track the conceivable hints of the intruder.

Watchdog and pathrater [51]: are presented for the DSR directing protocol. It is expected that wireless connections are bi-directional. Remote interfaces bolster indiscriminate mode operation, which implies that if a node A is inside the transmission scope of B, it can catch interchanges to and from B regardless of the possibility that those correspondences don't specifically include A. The watchdog techniques distinguish getting rowdy nodes. A node may gauge a neighboring node's recurrence of dropping or misrouting packets, or its recurrence of invalid routing data promotions. The execution of a watchdog is keeps up a cushion of as of late sent packets and contrasts each caught packet and the packets in the support to check whether there is a match. On the off chance that there is a match, the node expels the packet from the support. Generally if a packet has stayed in the cushion for longer than a specific timeout, the watchdog augments a disappointment count for the neighboring node. In the event that the count surpasses a specific threshold data transfer capacity, it makes an impression on the source advising it of the getting out of a node act with misbehavior way.

The shortcomings of watchdog are that it won't not recognize a getting into mischief node due to questionable impacts, beneficiary crashes, restricted transmission power, false conduct, intrigue, and incomplete dropping.

In another scheme, pathrater is executed by every node. Every node monitors the dependability rating of each known node, including ascertaining path measurements by averaging the node appraisals in the way to each known node. In the event that there are different path to a similar goal, then as per standard DSR routing protocol the briefest path in the course store is picked, although when utilizing pathrater the path with the most astounding metric is picked.

The watchdog components that recognizes getting into mischief nodes in MANET, intending to enhance network throughput with the nearness of narrow minded or vindictive nodes, the pathrater systems enhance network throughput, likewise assists the routing protocol with avoiding these egotistical or malevolent nodes.

*TWOACK [52]***:** to fathom these issues in the watchdog system, numerous researchers presented enhanced IDSs. Which is a standout amongst the most essential commitments in intrusion detection techniques.

The thought is to let each three continuous node to check whether the sent packet has been gotten by the node that is two hops far from it. This is accomplished by utilizing affirmation packet called TWOACK. TWOACK scheme can be included into source routing protocols such as DSR. TWOACK improves watchdog by taking care of the issue of identifying mischief nodes within the sight of impacts and restricted transmission control, although it is as yet defenseless against false rowdiness assault.

AACK [53]: is another imperative IDS uniquely intended for MANETs. It is an acknowledgement-based scheme at the network layer which can be considered as a blend of TWOACK and end-to-end affirmation scheme. By the presentation of versatile scheme, AACK extraordinarily decrease the system overhead when no mischief is identified when contrasted with TWOACK.

Host Based IDS: Shakshuki et.al [54] presented local IDS named *Enhanced Adaptive Acknowledgment (EAACK).*

For MANETs, the solution addresses a portion of the shortcomings of the Watchdog conspire, to be specific, false misbehavior, constrained transmission power, and collector collision. The IDS keep assailants from starting manufactured affirmation assaults by consolidating advanced mark in each message. This proposition depends on the affirmation scheme in which the goal node (D) is required to send an affirmation packet back to the source node(S). To defeat the danger of assailants sending manufactured affirmation packets the author presented the utilization of digital signature. All affirmation packets are carefully marked before they are conveyed to be confirmed by the goal. The model additionally executes a mechanism to find when a misbehavior report is started by an aggressor to harm the operation of the system. At the point when a node gets a report that another node is acting mischievously it runs a confirmation plan to affirm the report by making an impression on that node through an another route. One of the downsides in this arrangement is, it requires cryptographic keys to be dispersed ahead of time however it doesn't present any key exchange strategy. Another impediment is the way that digital marks present expansive system overhead which could be lessened utilizing other cryptographic strategies.

Cluster-based intrusion Detection technique [38]:

Intrusion recognition architecture for the impromptu systems has been discussed in the past part, which was initially introduced by Zhang et al. Nonetheless, the greater part of the nodes in this system should partake in the helpful intrusion detection exercises when there is such a need, which cause enormous power utilization for all the taking an interest nodes. Because of the restricted power supply in the ad hoc network, this structure may bring about a few nodes carry on greedy and not helpful with different nodes in order to spare their battery power, which will really abuse the first aim of this agreeable intrusion recognition architecture. To take care of this issue a cluster based intrusion identification strategy is utilized as a part of this method. A MANET can be composed into various cluster such that each node is an individual from no less than one cluster, and there will be just a single node for every cluster that will deal with the checking issue in a specific timeframe, which is by and large called cluster head. A cluster is a gathering of nodes that dwell inside a similar radio range with each other, which implies that when a node is chosen as the cluster head, the majority of alternate nodes in this group ought to be inside 1-hop region. It is important to guarantee the reasonableness and productivity of the cluster determination prepare. Here reasonableness contains two levels of implications, the likelihood of each node in the cluster to be chosen as the cluster head ought to be equivalent, and every node ought to go about as the cluster node for a similar measure of time. Proficiency of the procedure implies that there ought to be a few techniques that can choose a node from the cluster occasionally with elevation effectiveness.

2.2.2 Cooperation Enforcement

In MANET, an agreeable intrusion recognition architecture for ad hoc network, which was initially introduced by Zhang et al. all of the nodes in this structure should partake in the helpful intrusion detection activities, subsequently such a participation is critical to bolster the fundamental elements of the network. So there are three mechanism, were produced to uphold collaboration. Publicly, there are two sorts of getting out of misbehaving nodes, one is the greedy node, and the other is the malevolent node. Greedy nodes don't collaborate for greedy reasons, for example, sparing force. Despite the fact that the selfish nodes don't expect to harm different nodes, the fundamental danger from egotistical nodes is the dropping of packets, which may influence the execution of the system seriously. Malevolent nodes have the goal to harm different nodes, and battery sparing is not a need. With no motivating force for participating, network execution can be extremely debased. The systems to authorize coordinating are right now split into three research territories, token-based, micro-payment, and reputation-based. Yang [55] presented a token-based plan. Buttyan [40] presented the nuglets method. The nuglets method is small scale installment scheme. Buchegger's CONFIDANT [21], Michiard's CORE [32], and S.Bansel's OCEAN [30] are notoriety based scheme.

2.2.2.1 Token-Based Mechanism

The token-based technique [55] is a bound together network layer security arrangement in MANET in light of the AODV protocol. In this method, every node conveys a token keeping in mind the end goal to take an interest arrange operations, and its nearby neighbors cooperatively screen any bad conduct in directing or packet sending administrations. The approach is not quite the same as a watchdog, which screens neighbors alone, not cooperatively. Nodes without a substantial token are disengaged in the system, and the majority of their real neighbors won't collaborate with them in directing and sending administrations. Endless supply of the token, every node restores its token through its neighbors. The lifetime of a token is identified with the node's conduct. A well acting node with a decent record needs to restore its token less frequently. This approach utilizes asymmetric cryptography aborigine, for example, RSA. There is a global secret key and public key combine. Every authentic node conveys a token stamped with a lapse time and set apart with a mark. The outline depends on a few suppositions to streamline the mechanism: Any two nodes inside transmission range may screen each other, the approach is just in view of network layer security, not physical layer or link layer issues, just the safe course for information sending between the

source and goal is talked about, not information packet privacy and integrity, every node has a one of a kind ID, numerous aggressors are conceivable, however there is a cutoff to assailants in any area, and each real node has a token marked with the framework secret key, which can be checked by its neighbors.

2.2.2.2 Credit-Based Technique

The nuglets scheme [40] is an approach undifferentiated from virtual currency. A node that devours an administration must pay the nodes that give the administration in nuglets. The blend of watchdog and pathrater can't consider any misbehavior nodes responsible, and getting misbehaving nodes are as yet ready to send and get packets. Nevertheless, in the nuglets conspire, a trespass node will be bolted out by its neighbors. That is greatly improved in reasonableness. Nuglets are intended to reproduce packet sending. The nuglets are identified with the counters in the nodes. The counter is kept up by a trusted and alter safe equipment module at every node. A packet satchel holds nuglets, which are contained in the packet. The packet satchel is shielded from unapproved alteration and separation from the first packet by cryptographic systems. The packet forward protocol is outlined on settled per hop charges.

2.2.2.3 Reputation-Based Mechanism

Confidant [21] propose an expansion to the routing protocol so as to recognize and disengage getting rowdy nodes. The protocol is intended to have the capacity to make collaboration reasonable. With CONFIDANT, every node has four parts, a screen, a notoriety framework, a trust chief, and a path director. The CONFIDANT approach adapts to MANET security, vigor, and decency by retaliating for vindictive conduct and cautioning partnered nodes to maintain a strategic

-distance from awful encounters. Nodes gain from their own understanding, as well as from watching the area and from the experience of their companions.

3. DISCUSSION AND FUTURE WORKS

Security is such a critical element, to the point that it could decide the achievement and wide set out of MANET. Security must be guaranteed in the whole framework including the security primitives, for example, protocol of key management, since general security level is dictated by the framework's weakest point. A great deal of research is still while in transit to distinguish new dangers and make secure systems to counter those dangers. More research should be possible on the vigorous key management framework, protocol which is trust-based, coordinated ways to deal with routing security, and information security at various layers. Here are some research points and future work in the zone:

Cryptography is the key security system utilized as a part of all parts of security. The quality of any cryptographic framework relies on upon appropriate key administration. Public key cryptography approach depends on the unified CA substance, which is a security frail point in MANET. A few papers propose to circulate CA usefulness to different or all system elements in view of a secret sharing scheme, while some recommend a completely dispersed trust demonstrate, in the style of PGP. Symmetric cryptography has calculation proficiency, although it experiences potential assaults on key ascension or key conveyance. For instance, the Diffie-Hellman (DH) methods is powerless against the man-in-the-middle assault. A lot of convoluted key exchange or appropriation protocol have been outlined, however for MANET, they are confined by a node's accessible resource, dynamic system topology, and constrained data transfer capacity. Productive key agreement and dispersion in MANET is a progressing research region.

Plurality of the present work is on preventive strategies with intrusion identification as the second line of protection. One intriguing examination issue is to assemble a trust-based framework so that the level of security requirement is subject to the trust level. Constructing a sound trust-based framework and coordinating it into the flow preventive techniques should be possible in future research. Because most assaults are flighty, a flexibility situated security arrangement will be more valuable, which relies on upon a multi-fence security methods. Techniques which is Cryptography-based offer a subset of methods. Different ways will be presented in research in the future.

4. CONCLUSION

Because of dynamic nature of MANETs and the missing of centralized feature makes such system more open to attacks. So, in this paper an overview of the different classifications of Defenses instruments to the specially appointed systems is presented. Management of key, Ad-hoc directing of wireless Ad-hoc systems were talked about as the proactive guard strategies and the intrusion framework as the responsive safeguards methods.

5. REFERENCES

[1] Zhang, Y., Lee, W., & Huang, Y. A. (2003). Intrusion detection techniques for mobile wireless networks. Wireless Networks, 9(5), 545-556.

[2] Pearlman, M. R., Haas, Z. J., Sholander, P., & Tabrizi, S. S. (2000, November). On the impact of alternate path routing for load balancing in mobile ad hoc networks. In Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing (pp. 3-10). IEEE Press.

[3] Zimmermann, P. R. (1995). The official PGP user's guide. MIT press.

[4] Luo, H., Zerfos, P., Kong, J., Lu, S., & Zhang, L. (2002, July). Self-securing ad hoc wireless networks. In ISCC (Vol. 2, p. 567).

[5] Patel, M. S. B., Solanki, M. K. H., & Patel, M. B. B. An Evolution of Different Layered based Attacks and Security Actions for Blackhole attack in Mobile Ad Hoc Network.

[6] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of applied cryptography. CRC press.

[7] Dalal, R., Singh, Y., & Khari, M. (2012). A review on key management schemes in MANET. International Journal of Distributed and Parallel Systems, 3(4), 165.

[8] Wu, B., Wu, J., & Dong, Y. (2009). An efficient group key management scheme for mobile ad hoc networks. International Journal of Security and Networks, 4(1-2), 125-134.

[9] Chan, A. F. (2004, March). Distributed symmetric key management for mobile ad hoc networks. In INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE

Computer and Communications Societies (Vol. 4, pp. 2414-2424). IEEE.

[10] Aziz, B., & Nourdine, E. (2008, April). A recent survey on key management schemes in manet. In Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on (pp. 1-6). IEEE.

[11] Anderson, R., Chan, H., & Perrig, A. (2004, October). Key infection: Smart trust for smart dust. In Network Protocols, 2004. ICNP 2004. Proceedings of the 12th IEEE International Conference on (pp. 206-215). IEEE.

[12] Anderson, R., Chan, H., & Perrig, A. (2004, October). Key infection: Smart trust for smart dust. In Network Protocols, 2004. ICNP 2004. Proceedings of the 12th IEEE International Conference on (pp. 206-215). IEEE.

[13] Yi, S., Naldurg, P., & Kravets, R. (2001, October). Security-aware ad hoc routing for wireless networks. In Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing (pp. 299-302). ACM.

[14] del Valle, G., & Cárdenas, R. G. (2005, January). Overview the key management in ad hoc networks. In International Symposium and School on Advancex Distributed Systems (pp. 397-406). Springer Berlin Heidelberg.

[15] Wu, B., Wu, J., Fernandez, E. B., Ilyas, M., & Magliveras, S. (2007). Secure and efficient key management in mobile ad hoc networks. Journal of Network and Computer Applications, 30(3), 937-954.

[16] Zhou, L., & Haas, Z. J. (1999). Securing ad hoc networks. IEEE network, 13(6), 24-30.

[17] Capkun, S., Buttyán, L., & Hubaux, J. P. (2003). Self-organized public-key management for mobile ad hoc networks. IEEE Transactions on mobile computing, 2(1), 52-64.

[18] Khalili, A., Katz, J., & Arbaugh, W. A. (2003, January). Toward secure key distribution in truly ad-hoc networks. In Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on (pp. 342-346). IEEE.

[19] Kapil, A., & Rana, S. (2009). Identity-based key management in MANETs using public key cryptography. International Journal of Security (IJS), 3(1), 1-26.

[20] Xiong, W. A., & Gong, Y. H. (2011). Secure and highly efficient three level key management scheme for MANET. WSEAS Transactions on Computers, 10(1), 6-15.

[21] Buchegger, S., & Le Boudec, J. Y. (2002). Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks. In Parallel, Distributed and Network-based Processing, 2002. Proceedings. 10th Euromicro Workshop on (pp. 403-410). IEEE.

[22] PushpaLakshmi, R., & Kumar, A. V. A. (2010). Cluster based composite key management in mobile ad hoc networks. Update, 4, 10.

[23] Sridhar, R., Mishra, S., & Balasubramanian, A. (2004). Hybrid Approach to Key Management for Enhanced Security in Ad Hoc Networks.

[24] Balasubramanian, A., Mishra, S., & Sridhar, R. (2005, March). Analysis of a hybrid key management solution for ad hoc networks. In Wireless Communications and Networking Conference, 2005 IEEE (Vol. 4, pp. 2082-2087). IEEE.

[25] Arabia, S. (2012). A Hybrid Schema Zone-Based Key Management for MANETs. Journal of Theoretical and Applied Information Technology35, 2.

[26] Velloso, P. B., Laufer, R. P., Duarte, O. C. M., & Pujolle, G. (2008, July). Analyzing a human-based trust model for mobile ad hoc networks. In Computers and Communications, 2008. ISCC 2008. IEEE Symposium on (pp. 240-245). IEEE.

[27] Balakrishnan, V., Varadharajan, V., Tupakula, U. K., & Lucs, P. (2007, June). Trust and recommendations in mobile ad hoc networks. In Networking and Services, 2007. ICNS. Third International Conference on (pp. 64-64). IEEE.

[28] Cho, J. H., Swami, A., & Chen, R. (2011). A survey on trust management for mobile ad hoc networks. IEEE Communications Surveys & Tutorials, 13(4), 562-583.

[29] Liu, Z., Joy, A. W., & Thompson, R. A. (2004, May). A dynamic trust model for mobile ad hoc networks. In Distributed Computing Systems, 2004. FTDCS 2004. Proceedings. 10th IEEE International Workshop on Future Trends of (pp. 80-85). IEEE.

[30] Bansal, S., & Baker, M. (2003). Observation-based cooperation enforcement in ad hoc networks. arXiv.

[31] Velloso, P. B. B., Laufer, R. P. P., Duarte, O. C. M., & Pujolle, G. (2008, August). A trust model robust to slander attacks in ad hoc networks. In Computer Communications and Networks, 2008. ICCCN'08. Proceedings of 17th International Conference on (pp. 1-6). IEEE.

[32] Michiardi, P., & Molva, R. (2002). Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Advanced communications and multimedia security (pp. 107-121). Springer US.

[33] Pinnaka, A. K., Tharashasank, D., & Reddy, V. S. K. (2013, February). Cost performance analysis of intrusion detection system in mobile wireless ad-hoc network. In Advance Computing Conference (IACC), 2013 IEEE 3rd International (pp. 536-541). IEEE.

[34] Husain, S., Gupta, S. C., Chand, M., & Mandoria, H. L. (2010, September). A proposed model for Intrusion Detection System for mobile adhoc network. In Computer and Communication Technology (ICCCT), 2010 International Conference on (pp. 99-102). IEEE.

[35] Mafra, P. M., da Silva Fraga, J., & Santin, A. O. (2012, March). A distributed IDS for ad hoc networks. In Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on (pp. 478-483). IEEE.

[36] Lin, H. C., Sun, M. K., Huang, H. W., Tseng, C. Y. H., & Lin, H. T. (2012, September). A specification-based intrusion detection model for wireless ad hoc networks. In Innovations in Bio-Inspired Computing and Applications (IBICA), 2012 Third International Conference on (pp. 252-257). IEEE.

[37] Selvamani, K., Anbuchelian, S., Kanimozhi, S., Elakkiya, R., Bose, S., & Kannan, A. (2012, May). A hybrid framework of intrusion detection system for resource consumption based attacks in wireless ad-hoc networks. In Systems and informatics (ICSAI), 2012 international conference on (pp. 8-12). IEEE.

[38] Boora, S., Kumar, Y., & Kochar, B. (2011). A Survey on Security Issues in Mobile Ad-hoc Networks. IJCSMS International Journal of Computer Science and Management Studies.

[39] Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 255-265). ACM.

[40] Buttyan, L., & Hubaux, J. P. (2001). Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks (No. LCA-REPORT-2001-011).

[41] Menaria, S., Valiveti, S., & Kotecha, K. (2010). Comparative study of distributed intrusion detection in ad-hoc networks. International Journal of Computer Applications, 8(9), 11-16.

[42] Anjum, F., & Mouchtaris, P. (2007). Security for wireless ad hoc networks. John Wiley & Sons.

[43] Li, Y., & Qian, Z. (2010, January). Mobile agents-based intrusion detection system for mobile ad hoc networks. In Innovative Computing & Communication, 2010 Intl Conf on and Information Technology & Ocean Engineering, 2010 Asia-Pacific Conf on (CICC-ITOE) (pp. 145-148). IEEE.

[44] Shen, H., & Li, Z. (2008, June). ARM: An account-based hierarchical reputation management system for wireless ad hoc networks. In Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on (pp. 370-375). IEEE.

[45] Sun, B., Wu, K., & Pooch, U. W. (2003, September). Alert aggregation in mobile ad hoc networks. In Proceedings of the 2nd ACM workshop on Wireless security (pp. 69-78). ACM.

[46] Li, G., He, J., & Fu, Y. (2008, June). A distributed intrusion detection scheme for wireless sensor networks. In Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on (pp. 309-314). IEEE.

[47] Wu, X., & Bertino, E. (2007). An analyasis study on zone-based anonymous communication in mobile ad hoc networks. IEEE Transactions on Dependable and Secure Computing, 4(4), 252-265.

[48] Nadeem, A., & Howarth, M. P. (2013). A survey of manet intrusion detection & prevention approaches for network layer attacks. IEEE Communications surveys and tutorials, 15(4), 2027-2045.

[49] Shakshuki, E. M., Kang, N., & Sheltami, T. R. (2013). EAACK—a secure intrusion-detection system for MANETs. IEEE Transactions on industrial electronics, 60(3), 1089-1098.

[50] Zhang, Y., & Lee, W. (2000, August). Intrusion detection in wireless ad-hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 275-283). ACM.

[51] Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 255-265). ACM.

[52] Liu, K., Deng, J., Varshney, P. K., & Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE transactions on mobile computing, 6(5).

[53] Shakshuki, E. M., Kang, N., & Sheltami, T. R. (2013). EAACK—a secure intrusion-detection system for MANETs. IEEE Transactions on industrial electronics, 60(3), 1089-1098.

[54] SakilaAnnarasi, R., & Sivanesh, S. (2014, May). A secure intrusion detection system for MANETs. In Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on (pp. 1174-1178). IEEE.

[55] Yang, H., Meng, X., & Lu, S. (2002, September). Self-organized network-layer security in mobile ad hoc networks. In Proceedings of the 1st ACM workshop on Wireless security (pp. 11-20). ACM.