I.J. Intelligent Systems and Applications, **2015, 03, 21-28**
Published Online February 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2015.03.03

Self Adaptive Trust Model for Secure Geographic Routing in Wireless Sensor Networks

P. Raghu Vamsi
Research Scholar, Dept. of CSE, Jaypee Institute of Information Technology, Noida, India
Email: prvonline@yahoo.co.in

Krishna Kant
Professor, Dept. of CSE, Jaypee Institute of Information Technology, Noida, India
Email: k.kant@jiit.ac.in

***Abstract*—** The presence of malicious nodes in the ad hoc and sensor networks poses serious security attacks during routing which affects the network performance. To address such attacks, numerous researchers have proposed defense techniques using a human behavior pattern called trust. Among existing solutions, direct observations based trust models have gained significant attention in the research community. In this paper, the authors propose a Self Adaptive Trust Model (SATM) of secure geographic routing in wireless sensor networks (WSNs). Unlike conventional weight based trust models, SATM intelligently assigns the weights associated with the network activities. These weights are applied to compute the final trust value. SATM considers direct observations to restrict the reputation based attacks. Due to the flexible and intelligent weight computation, SATM dynamically detects the malicious nodes and direct the traffic towards trustworthy nodes. SATM has been incorporated into Greedy Perimeter Stateless Routing (GPSR) protocol. Simulation results using the network simulator NS-2 have shown that GPSR with SATM is robust against detecting malicious nodes.

***Index Terms*—** Trust, Adaptive Trust Model, Security Attacks, Secure Routing, Intelligent Computing

I. Introduction

Mobile Ad hoc Networks (MANETs) and Wireless Sensor Networks (WSNs) are two special classes of wireless networks. WSNs are termed as the predecessor of MANETs. A WSN is composed of tiny and low-cost sensor nodes (SNs) having limited resources in-terms of processing, memory and energy. These networks are self configurable and the communication is carried using wireless links. Applications of these networks include temperature and humidity monitoring, pollution monitoring in environmental applications, supply chain management applications, body area networks, pressure and speed monitoring in automotive, pungent gas or chemical detection in industries, target detection in military etc. [1]. In general, these networks are deployed in open, unattended and hostile environments to monitor and report the events. Due to the openness of SNs in WSNs, they are subject to eavesdropping, physical tampering, etc., which leads to various security attacks. Research studies in MANETs have shown that packet delivery percentage can substantially decrease when malicious activities are present in the network. Cryptography methods can be utilized to mitigate security attacks posed by malicious nodes in the network and to provide authentication and secrecy. However, these methods require thousands of multiplication and addition operations to implement a single security operation. In addition, they are not efficient in identifying security attacks posed by an adversary from outside of the network. In other words, cryptography can aid communication security rather than routing security. Due to this reason, cryptographic methods are not suited for routing in resource constrained sensor networks.

A human behavior pattern called trust has been widely used by the researchers to aid routing security. Trust is the measure of belief by a node about the behavior of its neighboring nodes. This trust is formed by the assessment of cooperation and coordination received from the neighboring nodes in executing network activities such as packet forwarding, acknowledgements etc. [2]. The trust value of a neighboring node will be incremented by one unit if node exhibits the positive behavior. Otherwise the related trust value is decremented by one unit. Along with these trust values, special values called weights are assigned to network activities. Finally, a trust model computes absolute trust values of the neighboring node as the sum of products of weight and trust value of corresponding network activities.

A. Motivation

Static WSNs (SWSNs) and mobile WSNs (MWSNs) are two categories of WSNs. In SWSNs, nodes are fixed to their deployment positions throughout their operations. Whereas, in MWSNs nodes are facilitated with locomotion so that they are mobile in the network. In some cases, nodes are placed on the moving vehicles or tied to an animal so that the system experiences mobility in the network. The network operations in MWSNs are more complex as compare to SWSNs due to the unpredictable node mobility, use of wireless channels, lack of infrastructure, and so on. An important observation needs to be considered during mobility is that a node can discover new neighbors and its former neighbors can disappear. As the impact of malicious nodes is more on the network, a benign node can face more malicious and few benign nodes during its journey.

Copyright © 2015 MECS

Nevertheless, since a malicious node attempts to several attacks in various intervals and proportions in the network, the security mechanisms should be designed to predict the dynamics presented by malicious clients. Weights to service criteria (such as the number of packets forwards, network acknowledgement, packet integrity etc.) and their expectations need to be computed by considering such dynamics. In addition, the behavior assessment and its expectations computation of neighboring nodes should be systematic and correct in-order to forward the data packets to eligible trusted node. Moreover, the weights need to be computed intelligently so that a benign can not be assigned poor trust value. Intuition behind this is trust estimation becomes more precise when the weights are adaptable and the absolute trust values are correctly estimated. So, it is clear that a trust management system should be designed to support adaptive weights to service criteria and systematic computation of absolute trust using direct observations.

B. Contributions

Among the routing protocols, geographic routing offers guaranteed packet delivery in a dense network. These routing protocols perform routing based on the location information. A node forwards the packet to a node which is situated nearer to the destination. Whenever malicious nodes present in the network, they modify or tampers the packet integrity so that a benign node drops the packets as invalid. To mitigate such malicious activities, numerous researchers have developed trust models to facilitate routing protocols. Weighted statistical model to identify malicious nodes is presented in [3]. Reputation based trust models that compute total trust by combining direct and indirect trust opinions is proposed in [4-8]. Trust model based on the behavior of neighboring nodes has suggested in [9] [10]. In addition, heuristic frameworks for trust management have been evolved in recent years [11]. Most of these models apply weights to compute total trust value. However, these weights are heuristic assignments. There is no underlying mechanism to use such heuristic values. To overcome this limitation, a Self Adaptive Trust Model (SATM) is proposed in this paper. SATM intelligently assigns the weights to corresponding service criteria. In addition, SATM detects the malicious nodes dynamically and diverts the data packets towards eligible trusted nodes. SATM has been incorporated into Greedy Perimeter Stateless Routing (GPSR) protocol. Simulation results using the network simulator NS-2 have shown that GPSR with SATM is robust against detecting malicious nodes.

After explaining preliminaries and related work in Section II, network model and assumptions considered for SATM are presented in Section III. Section IV describes the SATM. Simulation study to validate the SATM is presented in Section V. Finally, Section VI concludes the paper.

II. Preliminaries and Related Work

A. Trust concepts

Trust is an abstract concept which has been widely used in various fields like psychology, sociology, anthropology, economics, political science, and computer science related fields such as e-commerce, social networks, cloud computing etc. [12] [28]. Trust in communication networks is defined as the degree of belief or confidence about the other nodes in the networks based on the past interaction and observations. Trust has several properties. First, Trust is not static, it is dynamic. Second, trust is asymmetric which means that two nodes may not have equal trust in each other. Third, trust is context dependent. The degree of trust will be built in context and application involved. The context or applications can be military surveillance, home automation, industrial applications, etc. Fourth, the trust is subjective. It has a quantifiable level or degree of belief over other nodes. Finally, trust is not transitive, which means that let "→" be the trust and A, B and C are three nodes, if A→B, B→C then A→C is not guaranteed [13]. The trust calculation and establishment are carried out in association with routing protocols. While performing routing, every node maintains a trust table which stores the observations of behavior of neighboring nodes to aid routing decisions. In a network, a node can obtain trust information either by direct observations or indirectly by collecting trust opinions of neighboring nodes in a distributed fashion or by receiving recommendations from trusted third parties in a centralized or hierarchical fashion. This trust value helps in mitigating potential risks such as dead or ambiguous paths and security threats. The trust value can be useful to circulate a warning or alarm message among friend nodes. In case, if the trust value is very low then the node will be isolated from the network

B. Greedy Perimeter Stateless Routing (GPSR)

Greedy perimeter stateless routing (GPSR) [23] is a geographic routing protocol which performs routing by identifying neighboring node that is close to the destination. GPSR works with extensive use of locations information of nodes in the network. It works in two modes: Greedy mode and perimeter mode. In Greedy mode, an efficient path will be identified to reach destination. In perimeter mode, the routes are identified along the perimeter of the region. This mode is used when greedy mode fails to find a path towards the destination. In addition, for routing decisions, GPSR maintains information related to distance of neighbors, link state of neighbors, and a path vector. All routing decisions are made with one hop information. The distance between neighbors is maintained through periodic beaconing location information. In mobile networks, a node may discover new nodes and its older neighbors can disappear. A fresh list of neighbors is maintained with periodic removal of dead nodes. A well known graph traversal rule called right hand traversal rule is employed in the protocol for perimeter forwarding of packets. During perimeter forwarding graph planarization techniques are used to avoid crossing lines in the network.

Copyright © 2015 MECS

A node identifies the state of the other node with the promiscuous use of the network interface. Both greedy and perimeter methods provide full GPSR protocol. Perimeter mode operates on planar graph when the greedy mode on a full network graph fails.

C. Related Work

There are several trust models which have been proposed in the literature to secure geographic routing. These models have been used in conjunction with GPSR protocol. A generic method to calculate trust by multiplying direct and indirect trust is proposed in [14]. This method considers the product of trust as reputation. Product of past actions and observations are considered as direct reputation. Let A and B are two agents, A needs to observe B for certain service s, at time t then the direct reputation of B is calculated as $DR_t\ A(B|s)=F_t\ (t,\ t_k)*\sigma_k$. Where, $F_t\ (t,\ t_k)$ is a time dependent function and σ_k is the number of positive observations. For each positive observation the value of σ_k will be incremented by one. Reputation will be calculated in a similar way by collecting information from friend nodes. Finally, total reputation is calculated as $TR = W_k * (DR_t\ A\ (B|\ s_k) + IR_t\ A\ (B|s_k))$. Where, W_k is the weight associated with service s_k. Trust concept has been included with Greedy Perimeter Stateless Routing (T-GPSR) in [16]. T-GPSR considers two service criteria: the number of packets forwarded (P_f) and number of packets forwarded without tampering (P_{wt}). The trust of a node is calculated as $T\ (n_i) = (W\ (P_f) * P_f + W\ (P_{wt}) * P_{wt})$. Where, $W\ (P_f)$ and W (Pwt) are the weights associated with two services.

In [17], weight is associated with a packet and the agent. An agent can forward the packet only if it has a trust value greater than trust associated with the packet. Some other related works can be found in [18]. All these models assume a heuristic weight to compute total trust. However, there is no underlying method to set heuristic values. To adjust the weights dynamically with respect to a variety of attacks posed by malicious nodes, a method has been proposed in this paper. This method computes total trust value by combining expectations associated with network activities and their corresponding weights.

III. Network Model, Adversary Model and Network Performance Metrics

A. Network Model and Assumptions

Let $S = \{s_1, s_2, \ldots, Sn\}$ be a set of sensor nodes in a sensor network, which are deployed in a geographical region (X_i, Y_i). The proposed model is designed with the following assumptions

- Each node in the network is aware of its identity and location information.
- Each node in the network holds a symmetric key to encrypt or decrypt the data packet.
- Each node in the network communicates using a bidirectional transceiver and makes use of promiscuous use of their network interface. In promiscuous mode, a node can observe all packets passing through its radio range.
- Each node periodically broadcasts a beacon message *<id, location>* to advertise the location information and its existence.
- Without loss of generality, every node in the network maintains a neighbor table which keeps track of neighboring node identities and corresponding location information. In addition to it, every node maintains a packet buffer table which stores a copy of all outgoing data packets and forwarding node identity.

The above assumptions hold in real environments. The works [23] [14-17] [31], also have made these assumptions for their proposals.

B. Adversary Model

Wireless medium of communication, the unattended nature of network and sensor node limitations has left scope for an intruder to capture and tamper the nodes. Such tampered nodes are kept back in the field by an intruder such that such nodes exhibit deviated behavior from the regular network operations. Such deviated behavior can be result into security attacks. Such security attacks can be classified as follows [2] [5][29].

- *Black Hole:* In this attack, a malicious node attempts to drop all the packets that it supposed to forward.
- *Selfish behavior:* An attacker relies on routing points, such as gateways or routing junctions, so that, packets forwarded by sensor nodes will be simply dropped, there by packets never reach the destination.
- *Grey Hole:* It is a variant of the Black Hole attack in which a malicious node selectively forwards or drops the packets. In addition, a Grey Hole node can tamper the integrity of the packet so that the receiver node drop the packet as it is invalid.
- *On-off attack:* A malicious entity behaves well and worse alternatively so that they can remain undetected while causing damage in the network.
- *Modification attacks:* A malicious node modifies the packet integrity by tampering its unique code or hash code so that a receiving node discards the packet as invalid.

Since the geographic routing protocols are inherently free from Sink Hole and wormhole attacks, the above attacks are considered as some of the serious attacks on routing procedure. As assumed in [16], each node in the network will have an independent attack profile. That means, every node works in a non - colluding manner.

C. Network Performance Metrics

The following network performance metrics are considered to evaluate the efficiency of the proposed model.

- *Packet Delivery Fraction:* It is the ratio of the number of packets received by the destination node to the number of packets sent by the source node. This metric is important to check the dependability of the trust system.
- *Packet Forwards:* It is the number of data packets that are successfully forwarded by the intermediate nodes.

Copyright © 2015 MECS

- *Routing Load:* Routing load is the ratio of control packets to the data packets generated in the network.
- *Average Hop Count:* It is the mean number of hops that the data packets are traversed to reach their destination.
- *Energy Consumption:* It is the average energy consumed in the network.
- *Throughput:* It is the mean data bits sent per second in the network. This metric reflects the efficiency of the trust system in delivering the data packets from source to destination.

IV. Self Adaptive Trust Model (SATM)

Adaptive trust model comprises two components: 1) expectation assessment component, 2) weight assessment component.

A. Expectation Assessment Component

Each node maintains an agent which takes account of two groups of network activities; first, a group of activities related to the successful packet forwards, second, a group of activities related to maintenance of packet integrity. With observations on two groups the weight and expectations are assessed.

The first group activities (g_1) (related to successful packet forwards) are sincerity in packet forwards (g_{11}) and network acknowledgment (g_{12}). Sincerity in packet forward represents the cooperativeness shown in the routing procedure to route the packet towards the destination. The network acknowledgement represents sincerity in acknowledging packet reception and forward.

The second group activities (g_2) (related to maintenance of packet integrity) are sincerity in maintaining packet integrity or data integrity (g_{21}) and node authentication (g_{22}). Sincerity in data integrity deals with forwarding a packet to the next node without performing any modification. Node authentication represents the ability to prove its identity.

To assess the expectation of group network activities, Beta expectation has been applied. Each node will observe its neighbors to understand networking environment. With these observations, trust values of neighboring nodes are calculated. During interaction and observations with neighbors, a positive experience (α) is rated as 1 and a negative experience (β) is rated as 0. Reputation score is the expectation value of Beta probability density function (PDF) [21]. A Beta PDF denoted by $beta(p|\alpha,\beta)$ and can be expressed by using gamma function Γ.

$$beta(p\,|\,\alpha,\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha).\Gamma(\beta)}.p^{(\alpha-1)}.(1-p)^{(\beta-1)} \quad (1)$$

Where, p is first order probability variable and $0\le p\le 1, \alpha,\beta>0$. The function is with the restriction that the probability variable $p=0$ if $\alpha<1$ and $p=1$ if $\beta<1$. The expectation is given by $E(p)=\alpha/(\alpha+\beta)$. Where α,β are ratings of r positive and s negative outcomes with $\alpha=r+1$ and $\beta=s+1$. The PDF $beta(p|\alpha,\beta)$ is second order probability. The fist order variable p is continuous and $p\in[0,1]$. So, with the first order value p, PDF in Eq.(2) is very small hence meaning less. As a remedy to this situation one can make use of either $\int_{p_1}^{p_2} beta(p|\alpha,\beta)$ or simply by considering the expectation of p. A simple solution to compute the trust is by using expectation of p is given by.

$$E(p)=\frac{r+1}{r+s+2} \quad (2)$$

B. Weight Assessment Component

In general, trust on an object will be increased with the number of interactions happened with it. For every positive observation the trust will be increased and for every negative observation the trust value will be decreased. To obtain better trust value, a node needs to perform an adequate number of interactions with its neighbors to strengthen their trust opinions or to assess weightage. An agent computes the weight assessment component with the group activities as follows

$$W(g_i)=\frac{NOI(g_i)}{NOI(g_i)+1} \quad (3)$$

Where, NOI is the number of interactions made during observation of group g_i network activities for i=1, 2. The final trust values of first and second group activities are computed as the product of their weights and expectation values is given by

$$F_t(g_1)=W(g_1)*\prod_{i=1}^{2}E(g_{1i}) \quad (4)$$

$$F_t(g_2)=W(g_2)*\prod_{i=1}^{2}E(g_{2i}) \quad (5)$$

C. Calculating Absolute Trust Value

From Equations 4 and 5, the product of expectation values of subgroup activities is multiplied by the weight of the entire group. This means that any deviation in expectation values of subgroup activities or weight value results in change in final trust value of the corresponding group. In this way, the final trust value of corresponding groups is adjusted automatically based on the observations made by a node. With the final trust values of each group, the total trust value of a neighboring node is calculated as

$$TT=F_t(g_1)+F_t(g_2) \quad (6)$$

Every node in the network computes the total trust value of their neighboring nodes for every fixed time period called trust update interval (TUI). Updated neighboring nodes trust values will help in making correct routing decisions. Finally, during routing, a node forwards a packet to one of its neighboring nodes with highest absolute trust value by computing following equation [30]

Copyright © 2015 MECS

$$T_{\max} = \left(\frac{\sum_{i}^{n} TT(i)}{n} \right) - 0.1 \quad (7)$$

Where, T_{max} is the highest absolute trust value, *TT(i)* is the total trust value of neighboring node *i*. The T_{max} value is adjusted by subtracting 0.1 from the division of sum of trust values of neighboring nodes to the number of neighboring nodes. By this, SATM provides an opportunity to the recently converted malicious nodes. Finally, packets are forward to a node with highest trust value.

D. Example

An example is presented in this section to understand the working nature of the proposed SATM. Let *i* and *j* are the two sensor nodes which are neighbor to each other. Assume that entire time domain of each node is divided into fixed intervals (also called trust update interval (TUI)). Between two TUIs, node *i* observes the group activities of its neighboring node *j* and computes the total trust value for every TUI. During early stage of network, that is after node placement and bootstrapping, the initial values of two groups are $NOI(g_1) = 2$ (minimum two interactions between a neighboring node), $E(g_1) = 0.5$ (r = 0 and s = 0, no positive and negative observations, from Eq (3)), $NOI(g_2) = 2$, and $E(g_2) = 0.5$, such that the total trust of neighbor *j* is 0.5 (from Eq. (6)). It means that the probability of having trust in neighboring nodes during the early stages of network operations is not completely low or completely high, however, it is moderate. An analogy from basic probability theory is that the chance of the appearance of a Head when an unbiased coin was tossed is 0.5, which models the nonconformity of the occurrence. In the same way, final trust can be modeled in the early stages as a node believes another node with probability 0.5. This value is considered as normal trust level or trust threshold of any node in the network.

After some time of network operation, during a TUI Δt_i , let assume $NOI(g_1) = 10$, $NOI(g_2) = 8$, $E(g_{11}) = 0.71$, $E(g_{12}) = 0.57$, $E(g_{21}) = 0.33$ and $E(g_{11}) = 0.66$ such that the weights of two groups respectively are $Wt(g_1) = 0.90$ and $Wt(g_2) = 0.875$. With these weights and expectations, final trust values of two groups are $F_t(g_1) = 0.36$ and $F_t(g_2) = 0.109$. And the total trust value of neighboring node during TUI Δt_i is 0.469, which is lower than normal trust during the early stage of the network. It can be noted from the numerical values that any substantial deviation in the expectations will lower the total trust value drastically. In this, weight values cannot decide the total trust, but only good weight value with fair expectation values can only boost the total trust value of a node. Finally, for every TUI, nodes having total trust value above trust threshold will be given preference to forward data packets than any other node in the network.

An analogy is provided to understand this model further. Let a firm conduct employee recruitments for various posts, in which weightage is given in the posts and educational qualifications. There may be several applicants having essential qualifications are attending the interview such that selection of a candidate is based on the expectation of performance in the interview along with the weightage to his educational qualifications. A candidate may be eliminated from the selection even though he has good weightage because of poor expectation of performance in the interview. In a converse case, a candidate may be selected for the post due to the fair expectations of performance in the interview with normal weightage to his qualification.

So, with the number of interactions and expectation of each service criteria, SATM computes the weightage intelligently and this value will be applied in computing final trust value.

Trust update interval value is a vital component in deciding the total trust value of neighbors. This value should not be too long or too short, however, it should be moderate. It means that the total trust value has to be calculated after having adequate number of interactions with the neighboring nodes. Usually, this value is set between 4.5 seconds to 5.0 seconds. In this model, observations in one TUI are not carried forward to another TUI.

Table 1. Simulation Parameters

Examined Protocols	TGPSR and SATM
Simulation time	600 seconds
Simulation area	1500 x 300 meters
Number of nodes	50
Transmission range	250 meters
Mobility model	Random way point
Maximum speed	20 m/s
Traffic type	CBR over UDP
Maximum connections	15
Packet size	64 bytes
Packet rate	4 packets/second
Maximum malicious nodes	25

V. Simulation Study

A. Simultion Setup

The network simulator NS-2.35 [22] was used to simulate the SATM. This SATM has been incorporated into a well known geographic routing protocol called Greedy Perimeter Stateless Routing (GPSR) [23] protocol (see Section II B). The legacy code of GPSR [24] has been ported to NS-2.35 and, TGPSR and SATM have been built over it. Since SATM computes trust of neighboring nodes with direct observations, its performance is compared with a well known direct observation based trust computation model that has been incorporated into GPSR protocol (TGPSR) (see Section II C) against various network performance metrics mentioned in Section III C. Adversary model specified in section III has been put in place to test robustness of SATM. Detailed simulation parameters are provided in

Copyright © 2015 MECS

the Table 1. The simulations were conducted on 50 dynamic random node topologies, and mean values of the results are presented. The beacon interval was set as a random value between 0.5 and 1.0 second.

B. Result Analysis

Fig. 1 plots the delivery fraction. It is noted from the graph that the packet delivery has been increased substantially even in the presence of 50 percent of malicious nodes in the network. It is further noted that with SATM the packet delivery fraction has been raised by 25 percent as compared to TGPSR in the presence of 50 percent of malicious nodes. Since fresh value of total trust of neighbors is computed for every TUI, when a node has to forward the packets, it handover the packet to the neighboring node having trust value above trust threshold. It is because of the SATM ability to identify best trust node for every TUI and packet forwards to the trusted neighbors.

Fig. 1. Packet Delivery Fraction

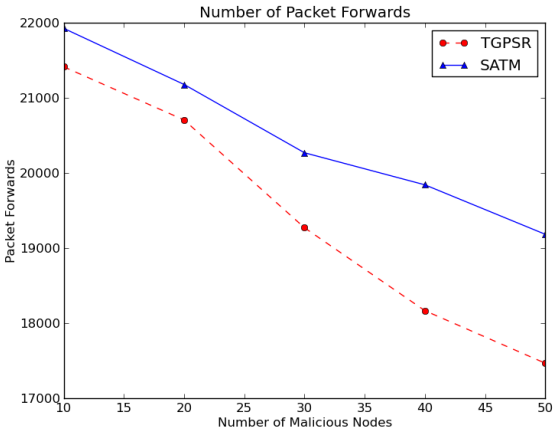

Fig. 2. Number of Packet Forwards

When the data packets are sent from the source, these packets are forwarded further towards destination by neighboring nodes or intermediate nodes between the source and destination. This metric can be defined as the number of packets forwarded by intermediate nodes between the source and destination in-order to reach the data packets to the destination. Fig. 2 shows the number of packets forwards in the network. It is observed that the number of packets forwards are high with SATM as compared to TGPSR since a node forwards the packet to the next eligible high trust value node instead of nodes in the shortest path. These forwards cause a packet to take additional paths than the shortest path. With this, the number packet forwards has been increased.

In a network, nodes communicate with two packets: 1) control packets, 2) data packets. The control packets are used to update node information such as node identity, node location, secret key information etc. Whereas data packets are actual data generated and sent by source nodes. Routing load is the ratio of control packets to the data packets generated in the network. Fig. 3 plots the routing load. It is noted from the Fig. that SATM with GPSR has lower routing load as compared to TGPSR protocol. This is because of the good packet delivery ratio achieved with SATM. With this, the number of control packets generated with respect to data packets is substantially decreased so that the routing load is also decreased.

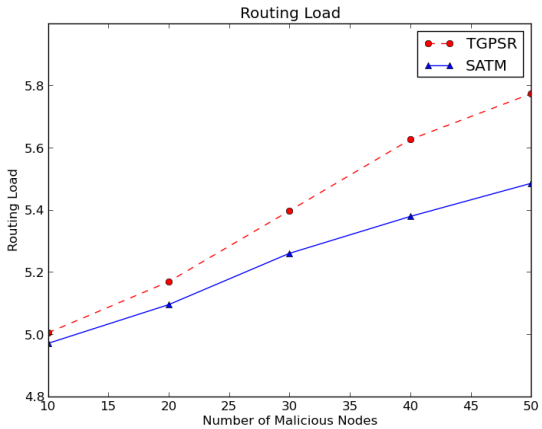

Fig. 3. Routing Load

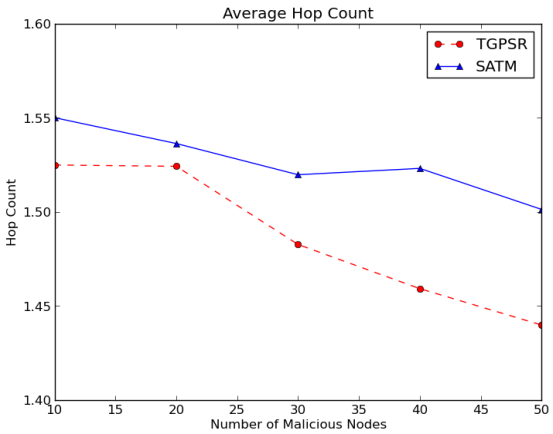

Fig. 4. Average Hop Count

Fig. 4 shows the average hop count. The graph shows that the average hop count of TGPSR has a sudden rise at 20 percent of malicious nodes and decreasing steadily till 50 percent of malicious nodes present in the network. By this, it can be interpreted that the TGPSR is dynamic in identifying alternate paths up to few malicious nodes

Copyright © 2015 MECS

present in the network and as the number of malicious nodes increases TGPSR is failed to find alternate paths. Whereas SATM is in a position to identify consistent routes even in the presence of 50 percent of malicious nodes in the network. Sudden peak in the SATM at 40 percent of malicious nodes indicates that it is more dynamic that TGPSR in identifying alternate paths as the number of malicious nodes increases in the network.

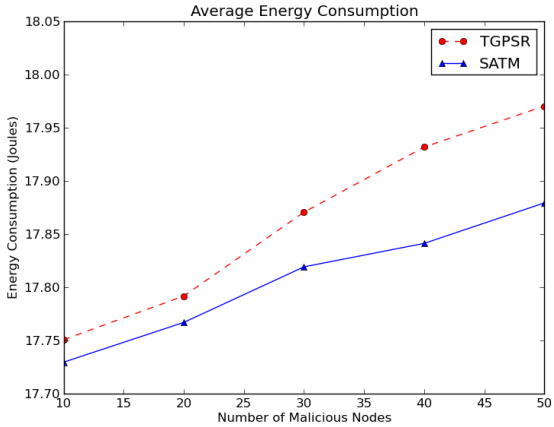

Fig. 5. Average Energy Consumption

The average energy consumed by nodes is directly proportional to the average energy consumed by the network. The average of energy consumed by all nodes in the network is the average energy consumed by the network. Fig. 5 plots the average energy consumed by the network. It is seen that this metric in SATM shows consistency in energy consumption as the number of malicious nodes in the network. It is further observed from the graph that the SATM require low energy consumption as compared to TGPSR. Nodes using SATM with GPSR consumed less energy since only neighboring nodes having total trust value greater than the trust threshold are considered for packet forwards. It can be observed from the graph that energy consumption is consistently increased from 10% to 50% of malicious nodes in the network.

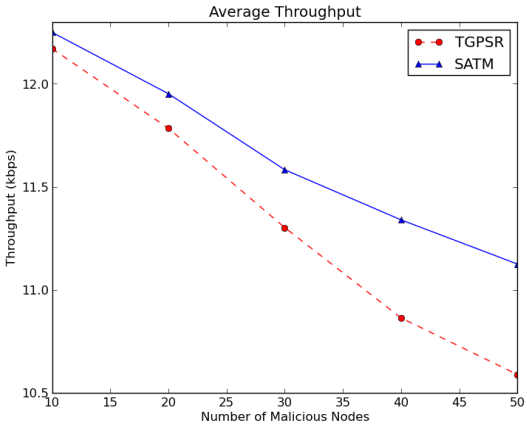

Fig. 6. Average Throughput

Fig. 6 plots the average throughput in the network. GPSR with SATM enables the nodes to increase the capability of suspecting a malicious node which drops or tampers the packets by updating the trust information for every TUI. It initiates a node to send data packets to the next trusted node to increase best-of-effort delivery. This results in increasing throughput with SATM as compared to TGPSR.

VI. Conclusion

A Self Adaptive Trust Model (SATM) for secure geographic routing has been proposed and implemented in this paper. The proposed SATM has been incorporated into Greedy Perimeter Stateless Routing protocol and validated its performance against various network performance metrics. Due to its flexibility in weights adjustments, SATM has dynamically identified malicious nodes and shown substantial improvement in packet delivery ratio, throughput, number of packet forward, end-to-end delay of packets etc. than a well known trust based GPSR (TGPSR) protocol. Finally, Simulation results show that SATM is robust against detecting malicious nodes.

References

[1] I.F.Akyildiz, W.Su, Y Sankarasubramaniam, E. Cayirci, ”Wireless Sensor Networks: A Survey”, Computer Networks, Elsevier, Pages 393-422, Volume 38, Issue 4, 15 March 2002.

[2] P. Raghu Vamsi and Krishna Kant, “Systematic Design of Trust Management Systems for Wireless Sensor Networks: A Review”, proceedings of ACCT 2014, 8-9 February, 2014.

[3] Probst, Matthew J., and Sneha Kumar Kasera. “Statistical trust establishment in wireless sensor networks”, Parallel and Distributed Systems, 2007 International Conference on. Vol. 2. IEEE, 2007.

[4] Urpi, A., M. Bonuccelli, and Silvia Giordano. “Modelling cooperation in mobile ad hoc networks: a formal description of selfishness”, WiOpt’03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks. 2003.

[5] Kuan Lun Huang, Salil S. Kanhere, Wen Hu, ”Are You Contributing Trustworthy Data? The Case for a Reputation System in Participatory Sensing”, proceedings of MSWiM10, October 1721, 2010.

[6] Saurabh Ganeriwal and Mani B. Srivastava, ”Reputation-based Framework for High Integrity Sensor Networks”, proceedings of SASN04, October 25, 2004.

[7] Suat Ozdemir, ”Functional reputation based reliable data aggregation and transmission for wireless sensor networks”, Computer Communications 31 (2008).

[8] Theodore Zahariadis, Panagiotis Trakadas, Helen C, Leligou, Sotiris Maniatis, Panagiotis Kar, ”A Novel Trust-Aware Geographical Routing Scheme for Wireless Sensor Net-works”, Wireless Personal Commun DOI 10.1007/s11277-012-0613-7, Springer, Published Online 15 April 2012.

[9] Huang, Lei, Lei Li, and Qiang Tan. “Behavior-based trust in wireless sensor network”, Advanced Web and Network Technologies, and Applications. Springer Berlin Heidelberg, 2006. 214-223.

[10] Theodore Zahariadis, Panagiotis Trakadas, Helen C, Leligou, Sotiris Maniatis, Panagiotis Kar, ”A Novel Trust-

Copyright © 2015 MECS

Aware Geographical Routing Scheme for Wireless Sensor Net-works", Wireless Personal Commun DOI 10.1007/s11277-012-0613-7, Springer, Published Online 15 April 2012.
[11] Huang, Lei, Lei Li, and Qiang Tan. "Behavior-based trust in wireless sensor network", Advanced Web and Network Technologies, and Applications. Springer Berlin Heidelberg, 2006. 214-223.
[12] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", proceedings of MOBICOM 2000, Boston MA, USA
[13] V. R. Sarma Dhulipala, N. Karthik, RM. Chandrasekaran "A Novel Heuristic Approach Based Trust Worthy Architecture for Wireless Sensor Networks", Wireless Personal Communications, DOI 10.1007/s11277-012-0688-1, 2012.
[14] Marcela Mejia, Nestor Pena, Jose L Munoz, Oscar Espanza, A Review of trust modeling in adhoc networks", Internet Research, Vol 19, issue 1, pp 88-104, 2010.
[15] Kannan Govindan, Prasant Mohapatra, "Trust computations and Trust Dynamics in Mobile Ad hoc Networks: A Survey", IEEE Communications Surveys and Tutorials, vol 14, No 2, Second Quarter 2012.
[16] M. Carmen Fern andez-Gago, Rodrigo Rom an, Javier Lopez, A Survey on the Applicability of Trust Management Systems for Wireless Sensor Networks", proceedings of Third International Workshop on SecPerU 2007.
[17] Michiardi, P. and Molva, R", CORE: A collaborative reputation mechanism to enforce node cooperation", proceeding of IFIP, 2002.
[18] AA Pirzada, C McDonald, "Trusted Greedy Perimeter Stateless Routing", proceedings of ICON 2007.
[19] Nael Abu Gazaleh, Kyoung Don Kang and Ke Liu, "Towards Resilient Geographic Rout-ing in WSNs", Proceedings of Q2Winter, Oct 13, 2005.
[20] Ka-Shun Hung, King-Shan Lui, and Yu-Kwong Kwok, "A Trust Based Geographical Routing Scheme in Sensor Networks", proceedings of IEEE WCNC, March 2007.
[21] Chen, Hongyang, et al. "Cooperative node localization for mobile sensor networks", Embedded and Ubiquitous Computing, 2008. EUC'08. IEEE/IFIP International Conference on. Vol. 1. IEEE, 2008.
[22] Yong wang, Garhan Attebury, Byrav Rammurthy, "A Survey of Security Issues in Wire-less Sensor Networks", IEEE Communication Surveys and Tutorials, 2nd Quarter, No 2, Vol 8, 2006.
[23] Audun Jsang, Roslan Ismail, "The Beta Reputation System", proceedings of 15th Bled Electronic Commerce Conference, Bled, Slovenia, June 17 - 19, 2002.
[24] Network simulator ns-2 available at: http://www.isi.edu/nsnam/ns/
[25] B. Karp and H. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," in Proceedings of the 6th Annual ICMCN, ACM Press, 2000, pp. 243–254.
[26] GPSR source code available at: http://www.icir.org/bkarp/gpsr/gpsr.html
[27] P. Raghu Vamsi, Payal Khurana Batra and Krishna Kant, "BT-GPSR: An Integrated Trust Model for Secure Geographic Routing for Wireless Sensor Networks", proceedings of 3rd IEEE Students Conference on Engineering and Systems, 28-30 May 2014.
[28] Sadra Abedinzadeh, Samira Sadaoui,"A Rough Sets-based Agent Trust Management Framework", IJISA, vol.5, no.4, pp.1-19, 2013.DOI: 10.5815/ijisa.2013.04.01
[29] Koffka Khan, Wayne Goodridge,"Impact of Multipath Routing on WSN Security Attacks", IJISA, vol.6, no.6, pp.72-78, 2014. DOI: 10.5815/ijisa.2014.06.08.
[30] Xiang, Ming, Quan Bai, and William Liu. "Trust-based Adaptive Routing for Smart Grid Systems." Journal of Information Processing 22.2 (2014): 210-218.
[31] P. Raghu Vamsi and Krishna Kant, " An Improved Trusted Greedy Perimeter Stateless Routing for Wireless Sensor Networks", International Journal of Computer Networks and Information Security, MECS Press, Vol. 6, No. 11, pp. 13-19, 2014.

Authors' Profiles

P. Raghu Vamsi is full time PhD research scholar in Department of Computer Science and Engineering (CSE), Jaypee Institute of Information Technology (JIIT), Noida, India, from the year 2012. He received B.E in CSE from University of Madras, Chennai, India, M.Tech in Software Engineering from Kakatiya University, Warangal, India, and M.B.A in Human Resource Management from IGNOU, New Delhi, India, during the years 2003, 2007 and 2010 respectively. Before joining JIIT, he has 7 years and 6 months of teaching experience in various engineering institutions. He is a student member of IEEE, ACM and life member of CRSI, ISTE India.

Krishna Kant, PhD., is Professor and Dean (Academic), Department of Computer Science and Engineering, Jaypee Institute of Information Technology, Noida, India. Earlier he served as Senior Director in the Department of Information Technology, Ministry of Communication and Information Technology, Government of India. He received his Masters in Physics (with specialization in Electronics) in the year 1972 from Jabalpur University, his Masters in Computer Science in the year 1975 from BITS Pilani, and his Ph.D. in Computer Science in the year 1980 from the Indian Institute of Technology Delhi. Dr. Krishna Kant has wide experience in designing and implementing microprocessor-based, real-time systems for different applications. He coordinated the UNDP project on Microprocessor Application Engineering Programme (MAEP) and was closely associated with the conceptualization and development of a number of agri-instrumentation systems at MAEP centre at JNKVV Jabalpur, India. He also imparted training to agriculture scientists on microprocessor applications. He taught "Microprocessor and Applications" and "Computer Control of Processes" courses to MCA and ME students, respectively, for three years in the University of Delhi, India. He has authored five books.

Copyright © 2015 MECS