International Journal of Engineering Studies.
ISSN 0975-6469 Volume 8, Number 2 (2016), pp. 187-197

http://www.ripublication.com

Trusted Secure Geographic Routing Protocol for Detecting Insider Attacks in MANET

Aruna Rao S.L.[1] and Dr. K.V.N. Sunitha[2]

BVRIT Hyderabad College of Engineering for Women,
Rajiv Gandhi Nagar, Nizampet Road, Bachupally, Hyderabad, India.

Abstract
In Mobile Ad hoc Network (MANET), the nodes are linked to one another wirelessly and are self sustaining. The member nodes of MANET are very robust and minute. The deployment and maintenance of this network is less expensive and comparatively easy when compared with the conventional networks. However, MANET is highly susceptible to attacks due to its infrastructureless topology. The possible attacks vary over a wide range and affect the network in different levels. To overcome these attacks and safeguard the network performance, in this paper we propose to develop a trusted secure geographical routing protocol for detecting insider attacks. This routing protocol determines the trust value of its neighbouring nodes and based on it, packets are transmitted. The neighbouring nodes are monitored to check if they forward the packets successfully or not. In this way, trustworthy nodes are recorded and the untrustworthy nodes are determined to be malicious. The malicious nodes are omitted from routing process.

INTRODUCTION

Mobile Ad hoc Network (MANET)

MANET is a self configuring network consisting of highly mobile member nodes which interact with each other. The network processing does not depend on any deployed infrastructure. The mobile nodes which are residing within the communication range of one another detect themselves and link wirelessly. When a node needs to communicate with another node which is not within its transmission range, then the intermediate nodes lying between the source and destination node, forward the packets to other intermediate nodes in the network till it is delivered at the destination. Thus, in MANET, the intermediate nodes work as routers [1].MANET is efficient in applications such as military, emergency purpose, etc due to its distributed topology [1]. The nodes in MANET are highly mobile in an unpredictable manner and are based on the flat geographical position data [2].

Attacks in MANET

Attacks in MANET are mainly due to the malicious nodes, which compromise the network node privacy and integrity. In this way, the performance of the network is hindered [3]. Some of the attacks possible in MANET are ,black hole or grey hole attack, Sinkhole attack, Replay attack, Link Spoofing attack, Modification attack, Sybil attack, Colluding node attack , Flooding attack.

Attack Prevention techniques in MANET

To overcome the attacks in MANET and to enhance the network performance, several routing protocols have been designed. Routing protocols such as Dynamic Source Routing protocols and BSD's ARP protocol are used to discover new secure routes and also solve the IP related issues [4]. Another way of avoiding attacks in MANET is by identifying valid nodes based on trust value. Inorder to achieve this, a trust management system is developed. In the trust management system, various characteristics of the network nodes are gathered, scrutinized and then used for deciding its validity [5].

RELATED WORKS

Payal Khurana Batra et al [6] have proposed BT-GPSR: An Integrated Trust Model for Secure Geographic Routing in Wireless Sensor Networks. The BT-GPSR model is developed by the combination of the weighted trust model as well as the beta reputation system. After employing this technique, the network features like throughput, number of packets transmitted, packet delivery ratio, hop count, etc have enhanced by a drastic range when compared with the traditional techniques. Based on the simulation results, it is proved that the proposed technique performs better than the beta model as well as the weighted trust models.

KunWang [7] have proposed A Secure Trust-Based Location-Aided Routing for AdHoc Networks. In the proposed technique, DBLAR is used in the reputation determination system to handle the security related issues like inability to protect the network data from attacks by the compromised nodes. The malicious nodes are detected based on their low trust value, which is calculated by the combination of the direct trust value and the recommendation trust values. The detected malicious nodes are then prohibited from packet forwarding operation. The simulation results prove that the proposed technique ensures security and better performance in the network. But, the overhead involved in this technique is higher.

Hui Xia et al [8] have proposed a Trust prediction and trust-based source routing in mobile ad hoc networks. This routing protocol is developed on the basis of the previous experiences and prediction technique according to the logic rules. The trust based source routing protocol (TSR) is designed as an extension to the reactive trusted routing protocol to which the prediction trust value of the node is given as the input.

P. Raghu Vamsi et al [9] have proposed a Self Adaptive Trust Model (SATM) for secure geographic routing. In this paper, the SATM is combined with the Greedy Perimeter Stateless Routing protocol and the resulting network operation is analyzed. SATM technique is successful in detecting the malicious nodes with the aid of its robustness with respect to weight adjustment.

Chen Lyu et al [10] have proposed an efficient and secure geographical routing (ESGR) technique against a series of attacks. The proposed ESGR technique ensures security by combining the associative one way hash function and the TESLA scheme. On the basis of the opportunistic mechanism, the broadcasting feature as well as the packet forwarding ability of the wireless links is used. The ESGR protocol protects the packets from the various attacks which compromises the packet by incorporating a single routing feature with the non centralized trust model. The ESGR technique is capable of withstanding the presence of the malicious nodes and also manages to achieve maximum throughput. However some delay is introduced in the network operation.

TRUSTED SECURE GEOGRAPHIC ROUTING PROTOCOL

Overview

In this work, as an extension to the previous works, we propose to design a Trusted Secure Geographic Routing Protocol for detecting insider attacks. In this protocol, direct trust value is being estimated for each node based on the parameters number of packets forwarded (P_f) and number of packets forwarded without tampering P_{wt}. Trust value of other nodes is computed for a fixed trust update interval (TUI) [9].

To further detect neighbour nodes dropping or selectively forwarding packets, the sender overhears the wireless channel to check whether the packet is actually forwarded by its selected next hop node [10]. Finally, the total trust value for node is produced by combining the location trusted information and direct trusted information.

Then the routing metric is represented in terms of the combined trust value such that nodes with lowest trust values are omitted from routing table.

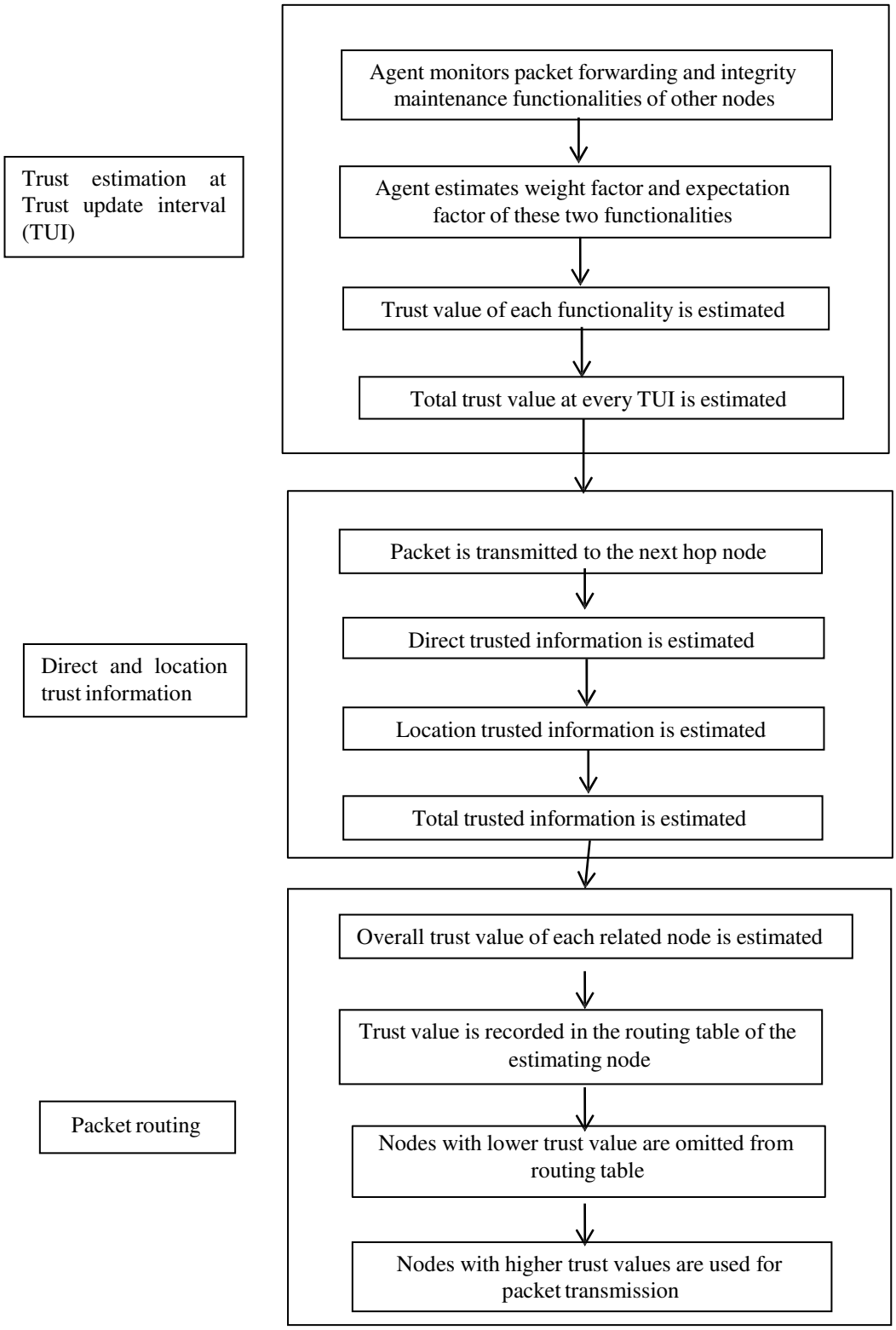

Figure 1: Block Diagram

Trust Value Estimation for Fixed TUI

In the network, each node maintains an agent. This agent is responsible for computing the trust value of the neighbouring nodes. The trust value estimation is based on the weight element and expectation element of two functionalities, namely packet forwarding function and packet integrity maintenance. During interaction and observations with neighbours, 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).

The trust value of the surrounding nodes is calculated by every respective node regularly at fixed trust update interval (TUI) [9]. This process is described in algorithm 1.

Algorithm 1
Notations:

1. F : Functionality
2. i : integer
3. $W(F_i)$: weight element of each functionality
4. NOI : Number Of Interactions
5. $E(F_i)$: Expectation element of each functionality positive
6. α : positive experience
7. β : negative experience
8. $T(F_1)$: trust value for the packet forwarding functionality
9. $T(F_2)$: trust value for the packet integrity maintenance functionality
10. $E(F_{11})$: Expectation value of sincerity in packet forward
11. $E(F_{12})$: Expectation value of network acknowledgment
12. $E(F_{21})$: Expectation value of sincerity in maintaining packet integrity
13. $E(F_{22})$: Expectation value of node authentication
14. TT_{TUI} : total trust value evaluated at fixed TUI

Algorithm:

1. The agent in each node in the network monitors its neighbour nodes to keep a check on the surrounding environment.
2. The agent estimates the weight element for each functionality, based on (1).

$$W(F_i) = NOI(F_i)/[NOI(F_i) + 1] \quad (1)$$

3. The agent estimates the expectation element for each functionality based on (2).

$$E(F_i) = \alpha / [\alpha + \beta] \quad (2)$$

4. Next $T(F_1)$ is estimated by the agent based on (3).

$$T(F_1) = W(F_1) * [E(F_{11}) + E(F_{12})] \quad (3)$$

5. Then the $T(F_2)$ is estimated by the agent based on (4).

$$T(F_2) = W(F_2) * [E(F_{21}) + E(F_{22})] \quad (4)$$

6. After the estimation of the trust value of each functionality, TT_{TUI} is estimated by the agent as

$$TT_{TUI} = T(F_1) + T(F_2) \quad (5)$$

7. The trust value estimated is recorded in the routing table of the node along with the other related information of the corresponding neighbour node.

This trust value information is recorded in the routing table and updated every TUI. In this way, the trust value of every neighbouring node is determined and recorded by each node in the network.

Trust Value Estimation based on Location and Direct Trust Information

After recording the trust information based on the weight and expectation factors, the packets are transmitted. After reaching the intermediate node, there are possibilities for the packet to get dropped. To determine if the packets are forwarded or dropped by the next hop node, the sender node overhears the wireless channel and based on the actions of the next hope node, its current trust value is computed. This process is described in algorithm 2.

Algorithm 2

Notations:

1. m : sending node
2. n : next hop node
3. P_f : number of packets forwarded
4. P_{wt}. : number of packets forwarded without tampering
5. DT_n : Direct Trust information of n

6. LT_n : Location Trust information of n
7. D_{mn} : distance between m and n
8. X_m : coordinates of node m's location
9. X_n : coordinates of node n's location
10. Ø : predefined constant
11. TT_n : total current trust value of n
12. $TT_{TUI(n)}$: total trust value of n evaluated at fixed TUI
13. TT(n) : overall trust value of n

Algorithm:

1. The node m forwards P_f to the next hop node, n.
2. On receiving P_f, n drops the tampered packets and forwards the remaining packets P_{wt}.
3. Through overhearing, m determines P_{wt}.
4. Then m estimates DT_n according to equation 6.

$$DT_n = P_{wt} / P_f \quad (6)$$

5. The node m estimates D_{mn} based on the signal strength since n is within the transmission range of m.
6. Then m compares D_{mn} with $\|X_m - X_n\| + ø$.
7. If $D_{mn} \leq \|X_m - X_n\| + ø$, then
8. $LT_n = 1$.
9. If $D_{mn} > \|X_m - X_n\| + ø$, then
10. $LT_n = 0$.
11. Trust value based on the overheard information and distance is combined to infer the TT_n according to equation 7.

$$TT_n = \eta . DT_n + (1-\eta) LT_n \quad (7)$$

where η is the factor with $0 < \eta < 1$.

12. Next the overall trust value is computed by adding the TT_n with the $TT_{TUI(n)}$ according to equation 8.

$$TT(n) = TT_n + TT_{TUI(n)} \quad (8)$$

13. The estimated TT(n) is then recorded in the routing table of m.

14. Every time a node transmits/ forwards a packet to its next hop node, it computes the TT and stores it in its routing table.
15. Intermediate nodes with lower TT are identified as malicious node or compromised node.
16. These malicious nodes are omitted from the routing table and hence not involved in further transmission of packets.

Thus, the packet is transmitted through the nodes with higher trust values. This enhances the successful transmission of packets, and in turn improves the overall network performance.

In this protocol, direct trust value is being estimated for each node based on the parameters number of packets forwarded (P_f) and number of packets forwarded without tampering P_{wt}

SIMULATION RESULTS

We use NS2 to simulate our proposed Trusted Secure Geographic Routing Protocol (TSGRP). We use the IEEE 802.11 for wireless sensor networks as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In our simulation, the number of nodes is varied as 20,40,60,80 and 100. The area size is 500 meter x 500 meter square region for 50 seconds simulation time, with Two Ray Ground Propagation, having Initial Energy 10.1J, transmission power 0.3 and receiving power 0.3. Nodes 1,2,3,4,5 Play the role of attackers. The simulated traffic is Constant Bit Rate (CBR).

Performance Metrics

We evaluate performance of the new protocol mainly according to the following parameters. We compare the ESGRP [10] protocol with our proposed TSGRP protocol.

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Energy Consumption: It is the amount of energy consumed for the data transmission.

Throughput: The throughput is the amount of data that can be sent from the sources to the destination.

Packet Drop: It is the number of packets dropped during the data transmission

Results & Analysis

The simulation results are presented in the next section. In our experiment we vary the number of nodes as 20,40,60,80 and 100.

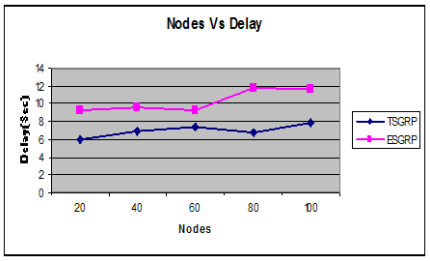

Fig 2: Nodes Vs Delay

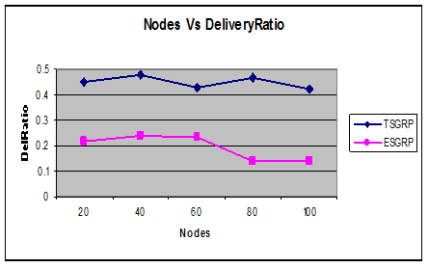

Fig 3: Nodes Vs Delivery Ratio

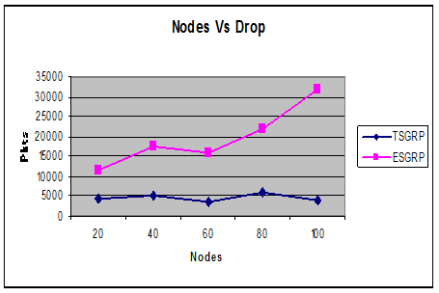

Fig 4: Nodes Vs Drop

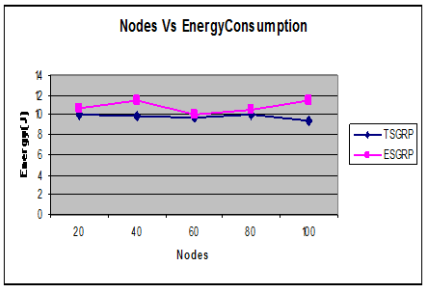

Fig 5: Nodes Vs Energy Consumption

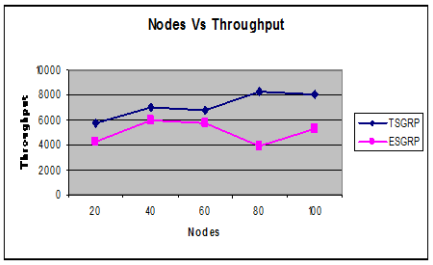

Fig 6: Nodes Vs Throughput

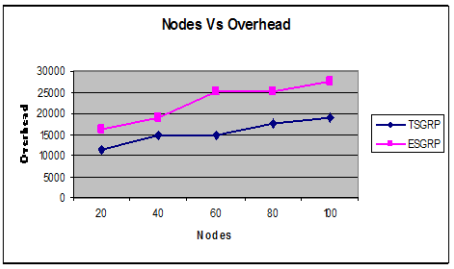

Fig 7: Nodes Vs Overhead

Figures 2 to 7 show the results of delay, delivery ratio, packet drop, energy consumption,throughput and overhead by varying the number of nodes from 20 to 100 for the CBR traffic in TSGRP and ESGRP protocols. When comparing the performance of the two protocols, we infer that TSGRP outperforms ESGRP by 32% in terms of delay, 57% in terms of delivery ratio, 74% in terms of drop, 9% in terms of energy consumption,28% in terms of throughput and 31% in terms of overhead.

CONCLUSION

In this paper, we have proposed a Trusted Secure Geographic Routing Protocol for detecting insider attacks in MANET. To overcome any attacks from insiders, in this protocol we select highly trustworthy nodes for packet transmission. The packets are routed through the secure geographic routes after determining the trustable nodes in the network. The overall trust value is estimated in two steps. Initially, the agent present in each node monitors all of its surrounding nodes and computes the trust value based on the two desired functionality at every Trust Update Interval (TUI). Then after the packets are transmitted to the next hop node, the transmitting node overhears the channel to determine the number of packets forwarded and dropped by the next hop node. Then according to the overheard information, the trust value of the next hop node is computed. Finally, the overall trust value of the neighbouring nodes is computed by combining the trust information obtained by overhearing the channel and trust value estimated at regular TUI. The trustworthy nodes are updated in the routing table and used for further packet transmission.

REFERENCES

[1] Hisham Dahshan, Fatma Elsayed, Alaa Rohiem, Aly Elmoghaz and James Irvine, "A Trust Based Threshold Revocation Scheme for MANETs", 978-1-4673-6187-3/13/$31.00 ©2013 IEEE.

[2] Mohamed Slim Ben Mahmoud and Nicolas Larrieu, "An ADS-B based Secure Geographical Routing Protocol for Aeronautical Ad Hoc Networks", Author manuscript, published in "IEEE COMPSAC 2013, 37th Annual International Computer Software & Applications Conference, Kyoto : Japan (2013)".

[3] Theodore Zahariadis, Panagiotis Trakadas, Helen C. Leligou, Sotiris Maniatis & Panagiotis Karkazis, "A Novel Trust-Aware Geographical Routing Scheme for Wireless Sensor Networks", Wireless Personal Communications, An International Journal, ISSN 0929-6212. Wireless Pers Commun DOI 10.1007/s11277-012-0613-7.

[4] Gavin Holland and Nitin Vaidya, " Analysis of TCP Performance over Mobile Ad Hoc Networks", Wireless Networks 8, 275–288, 2002. 2002 Kluwer Academic Publishers. Manufactured in The Netherlands.

[5] Guanghua Zhang, Yuqing Zhang, and Zhenguo Chen, "Using Trust to Secure Geographic and Energy Aware Routing against Multiple Attacks", PLOS ONE | www.plosone.org, October 2013 | Volume 8 | Issue 10 | e77488.

[6] Raghu Vamsi. P, Payal Khurana Batra and Krishna Kant, "BT-GPSR: An Integrated Trust Model for Secure Geographic Routing in Wireless Sensor Networks", arXiv:1406.3209v1 [cs.NI] 12 June 2014.

[7] KunWang, MengWu, Pengrui Xia and Subin Shen, "A Secure Trust-Based Location- Aided Routing for Ad Hoc Networks

[8] Hui Xia, Zhiping Jia, Xin Li, Lei Ju and Edwin H.-M. Sha, " Trust prediction and trust based source routing in mobile ad hoc networks", Ad Hoc Networks 11 (2013) 2096-2114, journal homepage: www.elsevier.com/locate/adhoc.

[9] P. Raghu Vamsi and Krishna Kant, "Self Adaptive Trust Model for Secure Geographic Routing in Wireless Sensor Networks", 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

[10] Chen Lyu, Dawu Gu, Yuanyuan Zhang, Tingting Lin, and Xiaomei Zhang, "Towards Efficient and Secure Geographic Routing Protocol for Hostile Wireless Sensor Networks", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Volume 2013, Article ID 491973,11pages, http://dx.doi.org/10.1155/2013/491973.