International Journal of Current Engineering and Technology

ISSN 2277 – 4106

Available at http://inpressco.com/category/ijcet

Research Article

Cross layer approach to detect malicious node inMANET

Vidya N. Patil[a*] and S.A.Thorat[a]

[a]Dept. of Computer Science and Enginnering Rajarambapu Institute of Technology, Rajaramnagar, India. 415414

Abstract

Mobile Ad hoc NETworks (MANET) are the wireless networks of mobile computing devices without any support of a fixed infrastructure. Routing in MANET is based on mutual support of nodes in the network. But some nodes from the network acts maliciously, so the routing in network collapses. Most security schemes suggested for MANETs tend to build upon some fundamental assumptions regarding the trustworthiness of the participating nodes and the underlying networking systems without presenting any definite scheme for trust establishment. For defining trustworthiness of the nodes different trust parameters are used by different authors in the literature. In order to calculate more accurate trust value we analyze these different parameters from network as well as MAC layer of protocol stack. Furthermore we also assign some weights to these parameters.

Keywords: *Trust, Trust parameters, Trust metrics.*

1. Introduction

[1]Mobile ad hoc network (MANET) is a set of mobile hosts which communicate among themselves by means of the wireless medium. Nodes from MANET forms network dynamically without help of any infrastructure and cooperate to forward data in a multi-hop manner without a central administration. MANETs were initially brought in for use in dangerous situations such as rescue and battle field operations so that emergency human resources or soldiers may be aware of the location of chemical, biological, hazardous material, or tactical situations. In such networks, all mobile nodes belong to a common authority (e.g., military or government agency) and are organized to collaborate with each other for a common goal. This type of MANET is termed as a *closed* or *managed* ad hoc network Routing in ad hoc networks has been an active research area and in recent years numerous routing protocols have been introduced for MANETs. The aim of routing in a MANET is to find out the most recent topology of a continuously changing network to find a correct route to a specific node. In the absence of any central organization system and shared wireless medium makes MANETs more vulnerable to different digital/cyber attacks. The attacks on the MANET are generally classified into two types: Passive Attacks and Active Attacks. Passive attacks are those that do not influence the functionality of a connection. Passive attack signifies that the attacker does not send any message, but just listens to the channel. If it is also possible for the adversary to interpret the captured data, the requirement of confidentiality is violated. Passive attacks are hard to detect because under such attacks as it does not produce any new traffic in the network, the network operates normally. In general, encryption is used to combat such attacks . On other hand, Active attacks are directed to change or destroy the data of a transmission or attempt to disrupt the normal functioning of the network. Active attacks when performed from foreign networks are referred to as external attacks. If nodes from within the ad hoc network are involved, the attacks are referred to as internal attack. Different security mechanisms are invented to overcome these attacks. One of the traditional approaches with the use of techniques like symmetric key encryption, digital signature and one way hash chain is cryptographic mechanism. Due to unavoidable shortcoming such as computational overhead, pre-establishment of keys we need to move towards another approach to provide security. Trust based mechanism is another way to provide the security to MANET routing. The concept of Trust originally derives from social sciences. Trust is defined as a belief level that one node can put on another node for a specific action according to previous direct or indirect information from observation of behavior.To understand trust management system we need to first understand basic definitions and concepts of trust management system.

Trust: Trust reflects the belief or confidence or expectations on the honesty, integrity, ability, availability and quality of service of target node's future activity/behavior . There are two types of trust

1. Direct trust which is associated with neighbors and it is first hand information.

*Corresponding author: **Vidya N. Patil**

2. Indirect trust which is associated with non-neighbors and it is second hand information. Trust Parameters: Behavior of node in the network activity which is used to decide trust level of node is called as Trust Parameter.

2. Related Work

Abusalah L, et al ; proposed a Trust-Aware Routing Protocol (TARP) for secure-trusted Ad-hoc routing. In TARP the trust routing scheme focusing on Quality of Trust. In TARP six security parameters are considered in computing the trust-level of a node in a given route and include: software configuration,hardware configuration, battery power, credit history, exposure and organizational hierarchy. A secure route is established based on a confidence level prescribed by a user in terms of these attributes. Bakar, A.A., et al , proposed a schema that can compute trust value among anonymous nodes to solve resource sharing problem. It uses Recommendation, Reputation, Knowledge, Observation and Context as trust parameters to calculate trust value of a node. Proposed schema computes a trust value to determine the access control privileges towards resource sharing. Wei Gong, et al; proposed a Trust mechanism in MANET based on Vector of Trust Model which is an abstract trust model. Here Packet forwarding ratio is used for trust calculation. Different weights are assigned to experience, knowledge and recommendation. In this mechanism each node should collect information from normal actions such as packet sending and receiving to compute its own trust vector about neighbor nodes. This trust vector can be normalized into a single trust value that has been provided as evidence for decision making in routing selection process. Shankaran, R. et al, highlighted the issues relating to trust in MANETs and describe a context-aware, reputation-based approach for establishing trust that assesses the trustworthiness of the participating nodes in a dynamic and uncertain MANET environment. Authors proposed a decentralized context-aware framework for building a trust model for MANETs. Here Device capability and Past performance together with their reputation used as parameters to calculate trust of a node. Weights are assigned to type of node ineraction as for direct experience weight assigned as, Weighting for direct experience WDE= 1, Weighting for observation, WO = 0.9 and Weighting for Indirect Experience (Recommendation), WIE= 0.8. Ferdous, R. et al; proposed schemes to formalize the notion of pair-wise trust between two nodes in an ad-hoc network. Packets sent by m to n that are dropped by m, Total packets dropped by m, Packets dropped by m due to congestion, Packets dropped by m due to unknown reasons,n’ s assessment of m’ s priority to m’ s self packets vs. all other nodes’ packets, Packet forwarding delay by m, Packets misrouted by m, Packets falsely injected by m are used as trust metrics. When a trusted one-hop neighbors move out of radiorange due to node mobility trust value decays exponentially. Xin Li et al; proposed a Trust-based Multipath Routing Framework for Mobile Ad Hoc Networks. In this framework weighted forwarding ratios and continued production rule are used to compute node trust and path trust respectively. Furthermore, adopting the trust model, author proposed a reactive routing protocol to find multiple trusted paths in one route discovery, which meet the dependable or trust requirements of data packets. Here both control packet forwarding ratio and data packet forwarding ratio are calculated for each node. Different weights are assigned to forwarding ratio of control packets and data packets. And Packet Forwarding Ratio is used as a trust metric. Fuzzy logic based approach is proposed by Ferdous R., et al;. Here two level fuzzy system is designed to decide the trust level of a node. First level will decide the percentage of packets dropped and second level will evaluate the trust level of the node. Percentage of packet dropped, Number of replay packets generated by this node, Number of false routing messages produced by this node, and Percentage of packets forwarded to wrong destinations are used as trust parameters. Aakanksha and Punam Bedi proposed MPRTAR, trust aware routing protocol based on the formation of trusted Mobile Process Groups(MPG).MPG-TAR calculate trust based on mobility rate, membership time within a local group and number of overlapping groups of a node. The proposed protocol continuously computes and updatesreliability, trustworthiness of a node and finds the confidence level in that node. If the node is trustworthy and reliable then confidence in that node is increased to trust the node for forwarding a data packet. In a scenario-based analysis is performed between Trusted Ad hoc On Demand Distance Vector Routing (TAODV) and Trusted Energy Aware Ad hoc On Demand Distance Vector Routing (TEA-AODV) with regard to fair treatment of trustworthy nodes by Burke, I.D. et.al. Numbers of packets received or sent to neighboring agents, remaining battery power are the parameters used for the trust calculations. TAODV uses Belief (b), Disbelief(d) and Uncertainty (u) triplets to make judgments about how it should respond to routing requests from various agents in the network. After studying different trust based systems we analyzed parameters used for trust calculation and trust calculation methods used by various researchers. After referring above papers, we decided to propose trust based system that will consider minimal set of parameters that will reflect node behavior not only at network layer but at other layers also. And to propose a trust formula to calculate the trust value of each node based.

3. Proposed Work

A. Motivation

Trust management is used to boost the security in MANET. To establish trust in the network we need to calculate trust value for each participating node. This trust value can be calculated by using different parameters which describes nodes behavior in the network. Trust parameters are nothing but the characteristics or behavior of the node in network. Different authors used different parameters to calculate the trust value. Also some

of which are assigned some weights to these parameters such that sum of weights of all parameters will equals to 1. Trust management can be application dependent and will be different based on the design goals of proposed scheme.

As we get from literature review, very few authors considered the attacks at multiple layers of protocol stack and proposed solution considering multiple layer parameters to overcome these attacks. So in this dissertation work are considering trust parameter that belongs to different layers of protocol stack.

B. Trust Formulation

In our approach we are considering Observation, Uncertainty, Experience, Recommendation and correctness of recommendation while calculating trust value for a node. So we derived a trust formula as:
T = W1 *O + W2*E + W3 R Where,
O: Observation
E: Experience
R: Recommendation
W1, W2, W3 --- Weights assigned to Observation, Experience, and Recommendation respectively.

1) Observation Calculation

For calculating Observation we considered 6 different parameters: Packet forwarding ratio, Delay in Forwarding, Back-off Time, Energy, Mobility, Normalized routing overhead. For each of this parameter we decided some threshold value. Calculating observation is based on direct observation and uncertainty. We use *Beta* distribution is initially employed to determine the prior trust relationship based on the past interactions. The Beta distribution is commonly used to model the evidence space. Due to its flexibility and simplicity Beta distribution is the most promising. Beta distribution is also simple to store as it is characterized by only two parameters. On the other hand, beta distribution is simple to store because it is characterized by just two parameters.
The observation is often described by two variables: α -- denoting the number of positive observations, and β -- denoting the number of negative observations. . Initially both α and β are set to 0. On each positive observation value of α is incremented by 1, while for each negative observation value of β is incremented by 1. Finally on having values for α and β we calculate observation O1 is calculated using Beta Distribution Function as:

$$O_1 = \frac{\alpha + 1}{\alpha + \beta + 2}$$

Here in above equation +1 term in the numerator and the +2 term in the denominator reduce the impact of sparse evidences.

2) Uncertainty Calculation

Uncertainty refers to the degree to which an individual or organization cannot accurately predict the behavior of its mutual rival or the environment. Uncertainty reveals whether a trustor has collected enough information from past interactions with a trustee and its confidence in that information . By using Feng Li, et al; definition of Uncertainty computation we calculated uncertainty (μ)as :

$$\mu 1 = \frac{12 * \alpha * \beta}{(\alpha + \beta)^2 (\alpha + \beta + 1)}$$

definition. First, when α+β is higher, it implies that there is more evidence, which consequently lowers uncertainty u according to the above definition. Second, when the evidence for success or failure dominates, there will be less uncertainty when compared to the situation in which there is equal evidence for both success and failure. This property is replicated by the fact that uncertainty u will be at its peak when α=β for any given (α+β). The numerator and denominator in above formula guarantee the latter and the former attributes, respectively. For value of either α or β equal to 0, value of μ1 also decreases to zero. To avoid this situation we calculated final uncertainty as exponential of above calculated μ1. So uncertainty is calculated as:

$$\mu = e^{\mu_1}$$

Therefore final value of Observation O is:

$$O = O_1 * \mu$$

3) Experience Calculation

Experience about a node is evaluated by directly monitoring packets communication of the node. This evaluation measures the ability of forwarding packets on node. Here Direct Experience is initialised to 0.5 i.e. a neutral experience. Then on receiving a experience value greater than 0.5 (positive experience) Direct Experience will be incremented by 0.1, on receiving a experience value less than 0.5 (negative experience) Direct Experience will be decremented by 0.1. Direct experience value ranges from 0 to
1. If a node has no past interactions Direct Experience is considered as neutral.

4) Recommendation Calculation

Simple Average scheme is used for recommendation calculation. Node A's evaluation to node B by collecting recommendations about node B from other nodes which should be the neighbor of node A.

5) Penalty Factor

On giving an incorrect recommendation a node is penalized by penalty factor. If node A has n neighbors average value recommendation of all n neighbors is calculated and each neighbors recommendation is checked for correctness against this average value. If

recommendation given by a particular node varies from average recommendation value by
0.2 then incorrect recommender will be penalized by multiplying its trust value by 0.8. i.e,

$$T_{inew} = T_{iold} * PF$$

Tinew — New Trust Value of node i.
Tiold — Old Trust Value of node i.
PF — Penalty Factor.
and ,

$$PF = \begin{cases} 0.8 & \text{if } |x - Ri| > \delta \\ 1 & \text{if } |x - Ri| \leq \delta \end{cases}$$

Where,
x — Average of Recommendations.
Ri — Recommendation provided by node i.
δ — Standard deviation of recommendation.

Trust Dynamics: Due to dynamic nature of the network it is considered that trust value of a node decayed with time. Then the time-dependent trust value is defined as follows:

$$T_{i_2} = T_{i_1} - (0.002 * \Delta t)$$

Where

Ti2— Trust Value of node i at time t2.
Ti1— Trust Value of node i at time t1.
Δt= t2- t1.

4. Result and discussion

A. Simulation Parameters:

We formed MANET simulation environment with 50 numbers of nodes. Some important parameters used in our simulation are given in Table 5.1 We used Random Waypoint mobility model to determine the node mobility and related attributes. We considered DSR as a base protocol for our implementation.

Table I. Simulation parameters

Total simulation time	200
Simulation area	1000 *1000
Total no of nodes	50
Maximum speed	20m/s
Pause time	10s
Data payload	512 bytes
Traffic type	CBR

We simulated the network with above parameters and constructed graphs of Packet Delivery Ratio, Throughput and Normalized Routing Overhead against No of malicious nodes in the network. Packet delivery ratio: It is the ratio of number of data packets successfully delivered to the destination to those numbers of data packets sent by source node.
Throughput: The average number of bits transmitted per second. Normalized Routing Overhead (NRO) : It is the total number of routing packets transmitted for each delivered data packet. Here in our simulation number of malicious nodes varies from 0 to 5, with a increment of one malicious node.

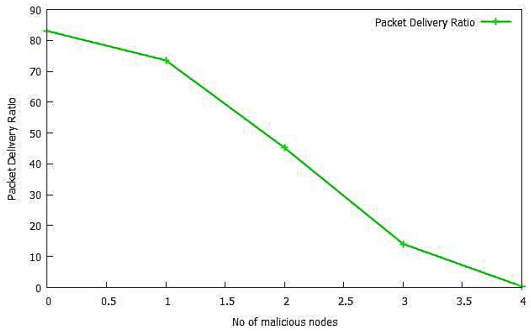

Fig. 1. No of malicious Nodes Vs PDR

Fig 1 shows that the packet delivery ratio is reduced slowly as the number of malicious nodes increases.

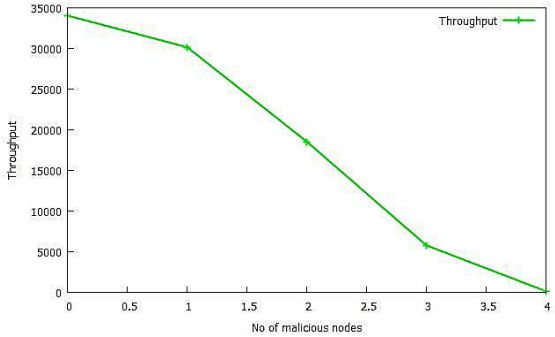

Fig. 2. No of malicious Nodes Vs Throughput

Fig 2 shows the impact of no of malicious nodes on control overhead.

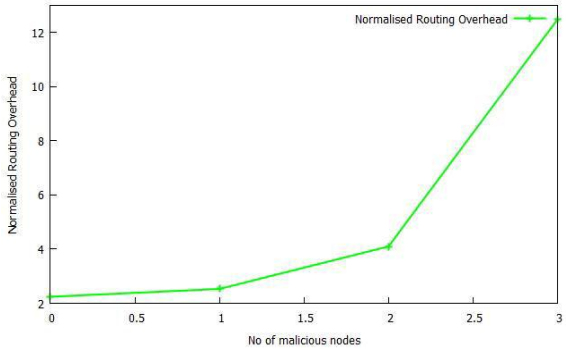

Fig. 3. Example of a figure caption. *(figure caption)*

Fig 3 shows as no of malicious nodes increases in the networkNormalized routing overhead increases. V.

Conclusion

We implemented a new trust based system to detect malicious node in MANET. We derived a new trust formula to calculate trust value considering Observation, Experience and Recommendation of node. We used beta distribution function to calculate the observation and uncertainty. We also considered the penalty factor to punish a node giving incorrect recommendations. On simulations with varying no of nodes we get Packet delivery ratio, throughput decreases while normalized routing overhead of network increases.

Future work

In future this work can be extended with adding some more trust parameters like Packet Integrity. Future work can also be done with isolating malicious node on detection from the network.

References

Lima, M.; dos Santos, A.; Pujolle, G , A survey of survivability in mobile ad hoc networks, Communications Surveys & Tutorials, IEEE , vol.11, no.1, pp.66-77, First Quarter 2009 doi: 10.1109/SURV.2009.090106

Younghwan Yoo; Dharma P. Agrawal; , Why does it pay to be selfish in a MANET?, Wireless Communications, IEEE , vol.13, no.6, pp.87-97, Dec. 2006 doi: 10.1109/MWC. 2006.275203

Dongbin Wang, Mingzeng Hu, Hui Zhi, A survey of secure routing in ad hoc networks, IEEE 2008.

Manoharan, R.; Mohanalakshmie, S.; , A trust based Gateway selection scheme for integration of MANET with Internet, Recent Trends in Information Technology (ICRTIT), 2011 International Conference on , vol., no., pp.543-548, 3-5 June 2011

Djahel, S.; Nait-abdesselam, F.; Zonghua Zhang; , Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges, Communications Surveys Tutorials, IEEE , vol.13, no.4,pp.658-672, Fourth Quarter 2011Jie Li; Ruidong Li; Jien Kato; , Future trust management framework for mobile ad hoc networks, Communications Magazine, IEEE , vol.46, no.4, pp.108-114, April 2008.

Govindan, K.; Mohapatra, P.; , Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey, Communications Surveys & Tutorials, IEEE , vol.PP, no.99, pp.1-20, 0 doi: 10.1109/SURV.2011.042711.00083

Abusalah, L.; Khokhar, A.; Guizani, M.; , NIS01-4: Trust Aware Routing in Mobile Ad Hoc Networks, Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE , vol., no., pp.1-5, Nov. 27 2006-Dec. 1 2006 doi:10.1109/GLOCOM.2006.264

Bakar, A.A.; Ismail, R.; Jais, J.; Manan, J.-l.A.; , Forming Trust in Mobile Ad Hoc Network, Communications and Mobile Computing, 2009. CMC '09. WRI International Conference on , vol.3, no., pp.470-474, 6-8 Jan. 2009.

Trust Based Malicious Nodes Detection in MANET 5138139

Wei Gong; Zhiyang You; Danning Chen; Xibin Zhao; Ming Gu; Kwok-Yan Lam; , Trust Based Malicious Nodes Detection in MANET, E-Business and Information System Security, 2009. EBISS '09. International Conference on , vol., no., pp.1-4, 23-24 May 2009 doi: 10.1109/EBISS.2009.

Shankaran, R.; Varadharajan, V.; Orgun, M.A.; Hitchens, M.; , Context- Aware Trust Management for Peer-to-Peer Mobile Ad-Hoc Networks, Computer Software and Application Conference, 2009. COMPSAC '09. 33rd Annual IEEE International , vol.2, no., pp.188-193, 20-24 July 2009 doi: 10.1109/COMPSAC.2009.132.

Ferdous, R.; Muthukkumarasamy, V.; Sattar, A.; , Trust Formalization in Mobile Ad-Hoc Networks, Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference on , vol., no., pp.351-356, 20-23 April 2010 doi: 10.1109/WAINA.2010.22.

Xin Li; Zhiping Jia; Peng Zhang; Haiyang Wang; , A trust- based multipath routing framework for Mobile Ad hoc NETworks, Fuzzy Systems and Knowledge Discovery (FSKD), 2010 Seventh International Conference on , vol.2, no., pp.773-777, 10-12 Aug. 2010 doi: 10.1109/FSKD.2010.5569349.

Ferdous, R.; Muthukkumarasamy, V.; Sattar, A.; , Trust Management Scheme for Mobile Ad-Hoc Networks, Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on , vol., no., pp.896- 901, June 29 2010-July 1 2010.

Aakanksha; Bedi, P.; , MPG-TAR: Mobile Process Groups Based Trust Aware Routing Protocol for MANETs, Advances in Recent Technologies in Communication and Computing (ARTCom), 2010 International Conference on , vol., no., pp.131-135, 16-17 Oct. 2010 doi: 10.1109/ARTCom.2010.

Burke, I.D.; van Heerden, R.; Olivier, M.S.; , Analysing the fairness of trust-based Mobile Ad hoc Network protocols: Comparing the fairness of AODV and TAODV protocols in scenario driven simulations, Information Security South Africa (ISSA), 2011 , vol., no., pp.1-8, 15-17 Aug. 2011 doi: 10.1109/ISSA.2011.

Yan Sun; Zhu Han; Liu, K.J.R.; , Defense of trust management vulnerabilities in distributed networks, Communications Magazine, IEEE , vol.46, no.2, pp.112-119, February 2008.

Feng Li; Jie Wu; , Uncertainty Modeling and Reduction in MANETs, Mobile Computing, IEEE Transactions on , vol.9, no.7, pp.1035-1048, July 2010.