www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13495-13498

A Novel Approach for Enhancing Security of MANET Using Trust Based Method

[1]Shabana M. L., [2]Anil K. Jacob

[1] M-Tech Student, Computer Science and Engineering, MES college of Engineering
Malappuram, Kerala, India
shabu9602@gmail.com

[2] Associate Professor, Computer Science and Engineering, MES college of Engineering
Malappuram, Kerala, India

Abstract: ***Mobile Ad-hoc Networks are a collection of two or more devices equipped with wireless communication and networking capabilities without a centralized infrastructure. The open medium and wide distribution of nodes make MANET vulnerable to attack from malicious nodes. In order to reduce the hazards from these malicious nodes, concept of trust is introduced in to the MANET. Trust Mechanisms secure data forwarding by isolating nodes with malicious intentions using trust value on the nodes. Different trust mechanisms are designed to enhance the security of MANETs. In this paper, the trust model has two components: trust from direct observation and trust from indirect observation. In direct observation, observer node directly evaluates the trust value of observed node based on its own opinion. In indirect observation, instead of taking arithmetic mean of trust values from all the neighbors, this method uses Dempster-shafer theory which provides a numerical measurement of degrees of belief about a proposition from multiple sources. As observer node needs to collects opinions from all its neighbors to evaluate the trust of observed node which is not in the range of observer node, it will cause congestion in the network. Thereby indirect observation takes some delay in trust value calculation. So selective deviation test and energy consumption filtering is applied to reduce delay in the network. By reducing the delay, packet delivery ratio in the network can be increased***.

Keywords: Manet, Security, Trust mechanism, Direct observation, Indirect observation, Energy consumption

1. Introduction

Mobile Ad Hoc Network (MANET) [1] can be described as an autonomous collection of mobile nodes (users) that communicate over relatively low capacity wireless links, with no support of any fixed infrastructure. In these networks, node movements and the wireless communication links may lead to dynamically changing and highly uncertain topologies. All network functions such as routing, multi-hop packet delivery and mobility management have to be performed by the member nodes themselves, either individually or collectively. So, network performance becomes highly dependent on cooperation of all member nodes. MANETs find applications in diverse fields ranging from low-power military wireless sensor networks to large-scale civilian applications and emergency search/rescue operations.

MANETs challenges
– Limited bandwidth
– Dynamic topology
– Routing Overhead
– Hidden terminal problem
– Packet losses due to transmission errors
– Mobility-induced route changes
– Battery constraints

Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain than in the wired network. Once the adversary is in the radio range of any other nodes in the mobile ad hoc network, it can communicate with those nodes in its radio range and thus join the network automatically. As a result, the mobile ad hoc network does not provide the secure boundary to protect the network from some potentially dangerous network accesses. Routing security is another critical problem in the security of Mantes, because there is no guarantee that all the nodes in a manet are connected in a one hop range. Secure routing based on trust in ad hoc networks is an important method for enhancing the security of Mantes.

Classes of approaches that can the safeguard tactical MANETs in the two methods: prevention based and detection-based approaches. One issue of these prevention-based approaches is that a centralized key management infrastructure is needed, which may not be realistic in distributed networks such as MANETs. Although prevention-based approaches can prevent misbehavior, there are still chances remained for malicious nodes to participate in the routing procedure and disturb proper routing establishment. Some excellent work has been done on detection based approaches based on trust in MANETs.

Trusting other people for the day to day transactions is inborn nature of human beings. In the mobile ad hoc network trust computation is useful in deciding the relay nodes in case of forwarding the packets. Trust management in MANET is highly challenging than in traditional centralized environments due to dynamic nature and characteristics of MANETs which creates difficulty due to change in topology and result in uncertainty and incompleteness. Trust management in MANETs is desired when a participating nodes wants a communication session and establish a network with satisfactory level of trust among themselves without any

previous interactions. In order to evaluate trust of nodes in Manets most research obtains evidence from two ways: direct observations (first hand information) and indirect observations (second-hand information). In MANETs direct observation occurs when an observer node collects evidence by interactions with an observed node directly. Indirect observations can be described when an observer node collects evidence of an observed node based on other node's verification.

2. Related works

Well organized surveys are available on trust based security enhancement in mobile adhoc network. D. Umuhoza et al. [2] proposed an Estimation of Trust Metric using Qos parameter and Source routing algorithm (ETQS). It provides a mechanism for finding the trust of communication path in an ad hoc network based on QoS parameters such as probabilities of transit time variation, deleted, multiplied and inserted packets, processing delays. This method is limited to specific cases where parameters of the environment are predictable. To see how the behavior of network traffic changes, sender and receiver share the information collected on network traffic in the form of a table and examine them. But this exchanging of tables containing traffic patterns between sender and receiver will cause traffic increase and therefore ETQS consumes more bandwidth.

S. K. Dhurandher et al. [3] proposed a Multipath and Message trust based routing (MMTR). MMTR uses a trust assignment and updating strategy which can be used to identify and isolate malicious nodes. This method considers the trust requirement of the message (T-Req) such that each message has a certain level of significance based on its content and type. T-Req decides how message will be routed and only path with certain trust level can be used for message forwarding. MTMR makes an assumption that each node should be able to detect the misbehavior and normal behavior exhibited by the neighboring nodes by working in promiscuous mode. When a message has a T-Req same as the trust level of the path then that message need not be encrypted and the message can be safely transmitted on that path. If a path of lower trust value has to be selected, the message should be broken into as many parts as is the value of T-Req and encrypted and sent on separate paths to preserve its contents from being revealed and modified. MTMR uses cipher-block chaining (CBC) mode of block encryption. Because of these encryption mechanisms, MTMR causes high overhead.

S. K. Dhurandher, et al. [4] proposed a Friend-Based Ad Hoc Routing Using Challenges (FACES). This method has been drawn from a network of friends in real life. It works by sending challenges and sharing friend lists to provide a list of trusted nodes to the source node through which data transmission finally takes place. The FACES algorithm is divided into four stages: Challenge Your Neighbor, Rate Friends, Share Friends and Route through Friends. The first three stages of the algorithm are periodic, while the fourth is on demand. The algorithm works by sending an initial challenge to provide authentication of nodes when no criterion is present initially. Nodes which have completed the challenge find place in the friend list. Nodes in the friend list are rated on the basis of the amount of data transmission they achieve and their friendship with other nodes in the network. The account of friendship of a node with other nodes in the network is obtained through the Share Your Friends process. One major benefit of this scheme is that the nodes do not need to promiscuously listen to the traffic passing through their neighbors. The information about the malicious nodes is gathered effectively by using challenges. This reduces the overhead on the network significantly. N. Marchang et al. [5] proposed a Light-Weight trust-based routing protocol (LWTR). This method is light weight in the sense that the Intrusion detection systems are used for estimating the trust that one node has for another. In this trust model, every node keeps a trust value for each of its neighbor. This value is a measure of the level of trust it has on its neighbor. This method considers only packet forwarding behavior of a neighbor in evaluating its trust level. LWRT is executed by every node in the network independently uses only local information thereby making it scalable. In order to obtain less biased trust value, opinions of neighbors are also considered in this method. LWRT simply takes arithmetic mean of every neighbor's opinion in trust evaluation. But it is not sufficient to reflect the real meaning of other unreliable observer's opinions.

3. Proposed work

In this section a new trust management system is introduced which is the enhanced version of the method, proposed by Z. Wei et al. [6]. In SMTU a trust management system that uses both direct and indirect observation to evaluate the trust of nodes in manet is brought up. It uses uncertain reasoning to derive trust value in both observations. Even though this method is efficient in many ways, but it takes longer trusted path from source to destination. The method proposed in this section is effectively overcome this problem.

The framework of the proposed system is explained as follows.

3.1 Trust from direct observation

In direct observation, observer node finds the trust value of observed node based on its own opinion. It makes an assumption that each observer can overhear packets forwarded by an observed node and compare them with original packets so that the observer can identify the malicious behaviors of the observed node. When a node receives a packet, the number of received packets, according to the type, will increase by one. If the node forwards the received packet correctly, the number of forwarded packets will increase by one. There are three scenarios that the number of received packets will not increase. Firstly, if the packet is dropped because of time to live (TTL), then the number of received packets should not increase. Secondly,if a node that drops a packet due to overflow of buffers. Thirdly, a packet is dropped by a node because the state of wireless connection is bad. Considering these significant factors, direct observation improves the accuracy of trust calculations. Here, the observer node estimates the trust values of its neighbors by using Bayesian inference. It is a type of uncertain reasoning which updates the belief about some hypothesis in the presence of new evidence. This scheme interpret trust as the degree of belief denoted by ɵ. ie, how much one node believes the other. The value of belief function ranges from 0 to 1. Bayesian inference derives posterior probability as a consequence of prior probability and likelihood function. Prior probability is the probability before some event has occurred or the data is observed and which is updated in the presence of new data or evidence to get the posterior probability. That evidence is the likelihood function. It also considers the past experience of a node in the trust calculation.

.

3.2 Trust from indirect observation

If we only consider direct observation, there is bias in the trust value calculation. So in order to obtain less biased trust value, verification from neighbor nodes are also considered. There are one-hop neighbors beside node B as shown in Fig. 1. Here node A is the observer node and node B is the observed node which is not in the radio range of node A. So node A calculates the trust value of node B by taking the verification from the common neighbors between node A and node B. Dempster-shafer theory is an approach for combining degree of belief derived from multiple common neighbors. Each common neighbor will give evidence to node A based on the observation about node B.

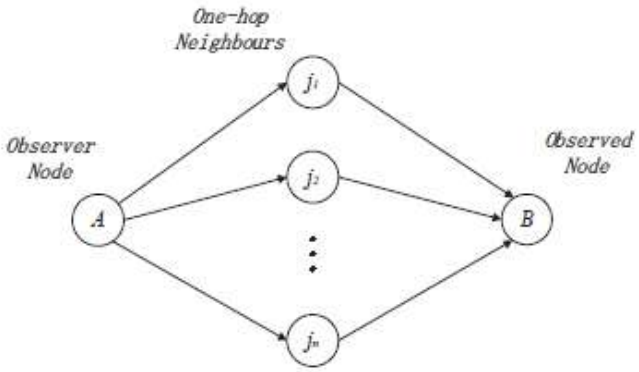

Figure 1: Framework of the proposed system

As observer node needs to collects opinions from all its neighbours to evaluate the trust of observed node which is not in the range of observer node, it will cause congestion in the network. Thereby indirect observation takes some delay in trust value calculation. So instead of taking all the neighbour's opinion, this approach selects only those nodes who successfully satisfies the following tests.

3.2.1 Selective deviation test

Selective deviation test is to ensure the unity of view with the receiving node point of view. In this test the observer compares each common neighbour's opinion against average trust value of all common neighbours. Here observer node calculates its own direct trust value for every common neighbours and compares against the average direct trust values all common neighbours. If $T_{ij}>T_{avg}$ where i is the observer node and j is one of the common neighbour, the observer node considers node j's opinion in trust evaluation. This enables fast reputation convergence which is critical in the challenged scenarios where nodes don't get enough time to observe the reputation of other nodes.

3.2.2 Energy consumption filtering

Energy consumption refers to how much energy is consumed by each node during packet transmission. When a node sends and receives packet, the networks interface of the node decrements the available energy according to the parameters: txPower and rcvPower represent energy usage for every packet antenna transmits and receives; txtime and rcvtime are time needed to transmit and receive a packet which calculated from packet size divided by bandwidth. By multiply transmit Power (txPower) with transmit time (txtime), we can know the amount of energy consumed during packet transmission. Here the observer node filters the common neighbours by using their energy consumption and filter out nodes that use more energy.

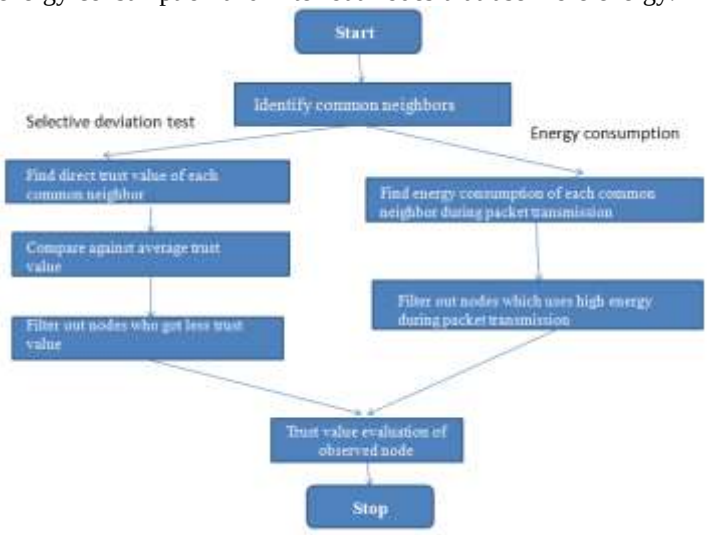

Fig.2 Framework of the proposed system

4. Results and Analysis

This work is done by using a well known network simulator(NS) version 2. NS-2 is a discrete event simulator for networking research and which works at packet level. For the simulation of this work nodes are placed randomly in the defined area by making the assumption that there are two types of nodes in the net- work: normal nodes, which follow the routing rules and compromised nodes, which drop or modify packets maliciously. The maximum velocity of each node is set from 0 to 10 m/s. The simulation area taken is 1000x1000 and maximum number of nodes is set to 70.

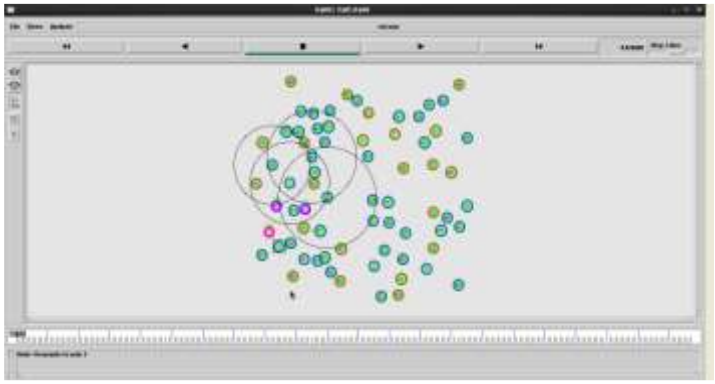

Figure 3: Mobile adhoc network scenario for 70 nodes

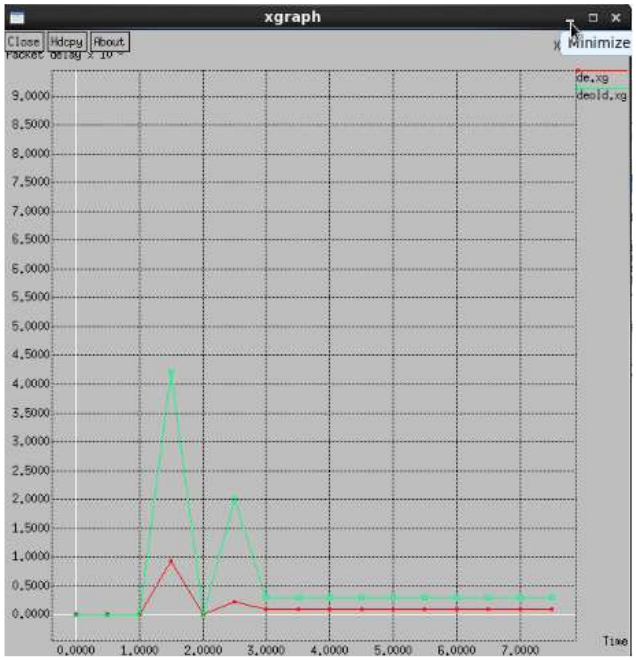

Figure 4: Average end to end delay comparison of SMTU and proposed method

Figure 5: Packet delivery ratio comparison of SMTU and proposed method

5. Conclusion

MANETs are vulnerable to different types of attacks due to its infrastructure less network. Different Trust based approaches are proposed to prevent such types of attacks and to enhance the security of MANETs. Trust is not a constant value, it changes over time. Uncertain reasoning is used in the trust management to derive the trust value of nodes accurately. This method interprets trust as the degree of belief that a node performs as expected. The trust model has two components: trust from direct observation and trust from indirect observation. With direct observation from an observer node, the trust value is derived using bayesian inference, which is a type of uncertain reasoning when the full probability model can be defined. On the other hand, with indirect observation, also called second hand information that is obtained from neighbour nodes of the observer node, the trust value is derived using the Dempster-Shafer theory, which is an approach for combining degree of belief derived from independent items of evidence. Instead of taking all neighbours opinion for trust calculation as in SMTU, this method filters the common nodes by using selective deviation and energy consumption filtering tests. The results of this filtering considerably improve the delay and packet delivery ratio.

References

[1] H. Yang, H. Y. Luo, F. Ye, S. W. Lu and L. Zhang, ”Security in mobile ad hoc net-works: Challenges and solutions,” *IEEE Wireless Communications, 2005*

[2]] D. Umuhoza, J. I. Agbinya and C. W. Omlin, ”Estimation of Trust Metrics for MANET Using QoS Parameter and Source Routing Algorithms,” *Proc. Second Int. Conf. on Wireless Broadband and Ultra Wideband Communications., 2007*

[3] S. K. Dhurandher and V. Mehra, ”Multipath and Message Trust-Based Secure Routing in Ad Hoc Networks,” *In In Proc. Int. Conf. Advances in Computing, Control and Telecommunication Technologies, pp. 189-194 ,2009*

[4]S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta and P. Dhurandher ”FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems,” Systems Journal, IEEE, 2011.

[5] N. Marchang and R. Datta, ”Light-Weight trust based routing protocol for mobile ad hoc net-works,” *In IET Information security, vol. 6, iss. 2, 2012.*.

[6]Z. Wei, H. Tang, F. R. Yu, M. Wang and P. Mason, ”Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning*,” IEEE Transactions on Vehicular Technology, 2014*.