ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Security Enhancement in Mobile Ad-Hoc Networks with Trust Management Scheme Using Uncertain Reasoning

Rajshree Ambatkar[1] , Smita Kapse[2] , Siddhi Raut[3] , Lalit Dole[4]

Assistant Professor, Department of CT, YCCE, Nagpur, India[1,2,3]

Assistant Professor, Department of CSE, G.H.Raisoni College of Engineering, Nagpur. India[4]

ABSTRACT: A mobile ad hoc network (MANET) is formed with wireless mobile devices without the need for existing network infrastructure. Security design in MANET is complicated because of its features including lack of infrastructure, mobility of nodes; dynamic topology and open wireless medium. Due to this MANET suffer from many security vulnerabilities. To enhance the security, it is very important to rate the other node which is trustworthy. Hence a unified trust management security scheme is used. Sometimes the knowledge in rules is not certain. Rules then may be enhanced by adding information about how certain the conclusions drawn from the rules. In trust management security scheme, the trust model has two components: direct observation and indirect observation. In direct observation, trust value is calculated from an observer node to observed node. On the other hand, indirect observation is also referred as secondhand information which is obtained from neighbor nodes of the observer node; the trust value is calculated between them. By combining these two components in the trust model using uncertain reasoning a more accurate trust value is obtained. This will help to improve throughput and packet delivery ratio in the network.

KEYWORDS: MANET, Security challenges, Trust Management, uncertain reasoning.

I. INTRODUCTION

A Mobile Ad Hoc Network is a type of ad hoc network that can dynamically change locations and self configuring on the fly. Because MANET consist of mobile nodes, they use wireless connections to connect directly or relying on other mobile node as router to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission [1]. In cases, where no network infrastructure exists, such as in war zones, relief efforts in remote territories, and emergency situations a mobile ad hoc network is used. Such network does not depend on pre-existing/centralized infrastructure and base stations. In decentralized network, all network activity including discovering the topology and delivering messages to the other nodes must be executed by the nodes themselves [2]. The applications for MANETs are diverse, ranging from small, static networks to large-scale mobile highly dynamic networks [1]. Other than application, MANETs need efficient distributed algorithms to determine network organization, link scheduling and routing [2][7]. The network protocol which is design for these networks is such a complex issue [2].

Open and closed are the two types of MANET's [1]. In open MANET, different nodes having different goals and they share their resources with each other for connecting globally. In closed MANET, all mobile nodes which are in networks cooperate with each other to achieve a common goal. MANET suffers from many security attacks Because of its distinct features including lack of infrastructure, node mobility, dynamic topology and open wireless medium [5]. Therefore, security is challenging issue in MANET [1]: Cryptography and key management schemes seem good [5], but they are too expensive in MANET. Prevention-based and detection based are the two approaches that are used in MANET [6]. In prevention-based approaches a centralized key management is required, which may not be possible in MANET because of its distributed networks. The whole network may be affected if the infrastructure is destroyed. So, this approach is used to prevent misbehaviour but not detect malicious nodes. Detection based approaches are used to detect selfish node that helps to identify malicious misbehaviour. Detection based approaches are based on trust in MANETs [3]. Hence this approach is used to calculate trust value in trust management schemes.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Most of the detection based approaches based on trust in MANETs, may not use both direct and indirect observation (second hand information obtained from neighbour node or third-party node). Trust evaluated from direct observation not able to differentiate data and control packets. For security in MANETs, it is important to identify nodes that are trustworthy to other nodes without using centralized authorities for building up a trust environment. Such mechanisms not only help to detect malicious node, but also improve network performance. For evaluating trust value, we are using both direct & indirect observation. In this paper, trust value calculation means degree of belief that is node performs as expected.

II. RELATED WORK

Unified Trust-based security schemes are very crucial detection-based system in MANETs, [1], the trust value of a node which is to be calculated based on direct observation using Bayesian methodology. In this paper use the concept of uncertain Reasoning (Uncertainty is unavoidable in everyday reasoning and in many real-world domains.) that the observed node performs a task correctly, and evaluate trust values by direct observation. Compared to direct observation in trust evaluation, indirect observation or second-hand information can be important to evaluate the trust of observed nodes. For example, the collection of evidences from neighbour nodes can detect the situation where a hostile node performs well to one observer, while performing poorly according to another node. The Dempster-Shafer theory (DST) is regarded as a useful mechanism in uncertain reasoning and is widely used in expert systems and multi-agent systems. In this paper, we use uncertain reasoning theory from artificial intelligence to evaluate the trust of nodes in MANETs. Uncertainty is an old problem from gambler's world. This problem can be handled by probability theory. In security in MANETs, we find that this theory is very suitable for trust evaluation base on the trust interpretation. Bayesian inference and Dempster-Shafer evidence theory are two approaches in uncertain reasoning. We adopt them to evaluate trust of nodes by direct and indirect observation.

III. PROPOSED ALGORITHM

The main goal of MANET is to establish trusted connection amongst each other. In detection based approaches, Unified trust management security scheme is one of the important methods [9]. By using trust information, node does not take highly risky action such as forwarding or sending the data packet to the node having low trust value. In trust management security scheme, trust model has two components: trust value which is calculated from direct observation & trust value calculated from indirect observation. In direct observation, trust value is calculated from an observer node to observed node. Indirect observation is also referred as second-hand information which is obtained from neighbour nodes of the observer node. Indirect observation or second-hand information is used to evaluate trust value of observed nodes from neighbour node. Indirect information is very important as Compared to direct observation. Example: information collected from neighbour nodes can able to detect situation where node's behavioural is well or not.

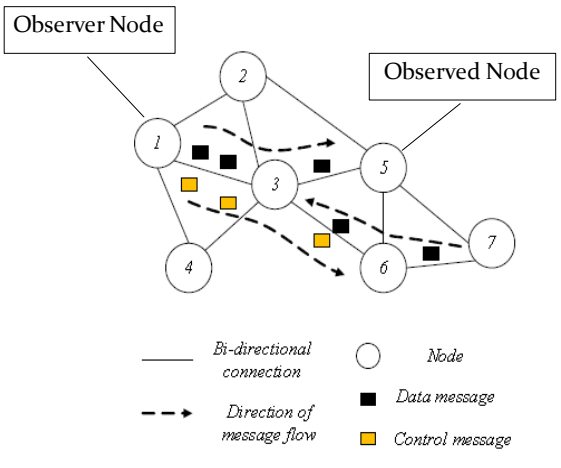

Fig 1: Mobile Ad hoc network

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

In this example, node 1 is an observer node and node 3 is an observed node. Node 1 sends data messages through node 3 to node 5. When node 3 forwards messages to node 5 then node 1 can observe the communication. Based on this observation node 1 can calculate the trust value of node 3. The same idea is applied to the control message situation. Meanwhile, node 1 can collect information from node 2 and node 4 to evaluate the trust value of node 3. This information collected from third party nodes is called indirection observation.

Table1: Abbreviations

Name	Definition
TAB	The total trust value that Node *A* gives Node *B*
TS	*AB* The trust value that Node *A* gives Node *B* based on direct observation of Node *A*
TN	*AB* The trust value that Node *A* gives Node *B* based on indirect observation of Node *A*
TD	*AB* The trust value that Node *A* gives Node *B* based on data packets
TC	*AB* The trust value that Node *A* gives Node *B* based on control packets
λ	The weight for the trust value based on direct observation
Γ	A factor of punishment which is larger than or equal to 1
P	The weight for the trust value based on data packets

IV. TRUST VALUE EVALUATION USING DIRECT OBSERVATION

Based on the model presented in the last section, evaluate trust values using direct observation on two malicious behaviours: drop packets and modify packets [4]. In the direct observation, we assume 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 behaviours of the observed node. Therefore, the observer node can calculate trust values of its neighbours by using Bayesian inference, which is a general framework to deduce the estimation of the unknown probability by using observation. As mentioned in the last section of trust model, Selfish or misbehaving nodes which are present in MANET can disrupt the working of network and degrade the performance of the network. Hence, it is very important to detect and remove these selfish nodes. Following are the various techniques available to prevent the selfishness in MANETs [4]:

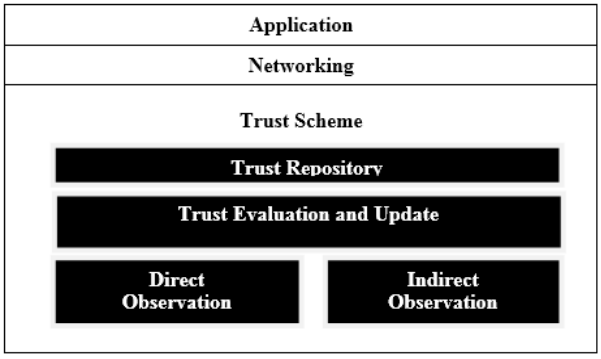

Fig 3 Trust Management Framework

V. TRUST VALUE EVALUATION USING INDIRECT OBSERVATION

Second Method is indirect observation used to evaluate the trust value of the observed node. Although direct observation from an observer is important in evaluating the trust value of the observed node, the evidences from

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

neighbour nodes are also helpful to judge the trustworthiness of the observed node. Collection of neighbour's opinions can help in justifying whether a node is unfriendly. This mechanism may reduce the unfairness from an observer. A situation in which a node is kindly to one node but malicious to others may be moderated. In order to implement this method, the Dempster-Shafer theory, which is a mathematical theory of evidence, is used as it is well developed for coping with uncertainty or ignorance, and it provides a numerical amount of degrees of certainty .The core of this theory is the certainty function that is based on two essential ideas: degrees of belief about a proposition can be obtained from subjective probabilities of a related question, and these degrees of belief can be combined together on condition .

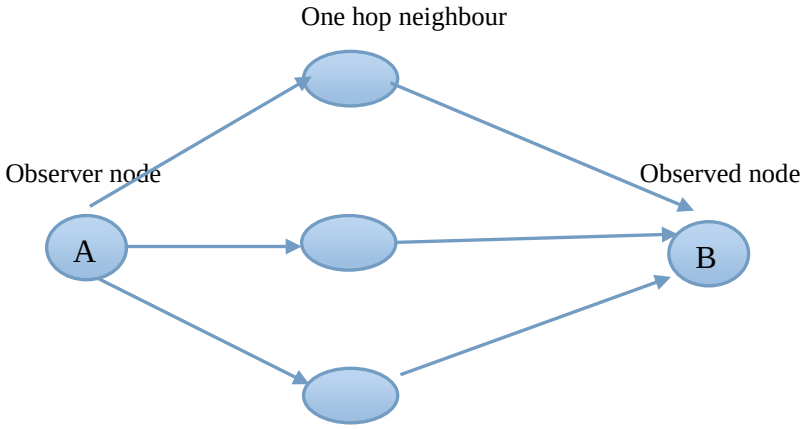

Fig 3 Indirect Observation

VI. SIMULATION RESULTS

- Trust Direct Observation text file is created a table for node 0 to node 29 which shows direct observation between nodes and showing their time, node id, degree of node and transmission is successful or not

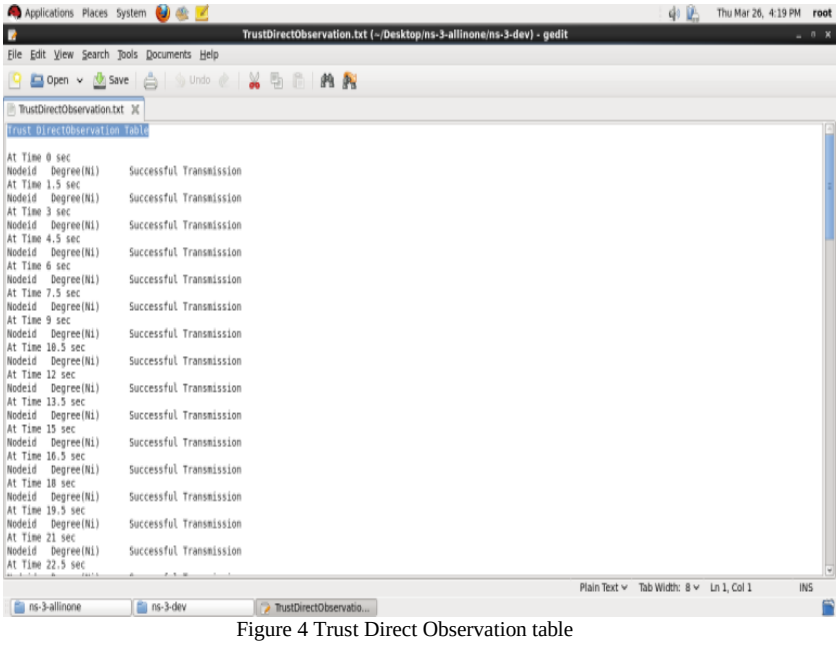

Figure 4 Trust Direct Observation table

- Two hop matrix is generated from that we can identify nodes i.e. two hop neighbors.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

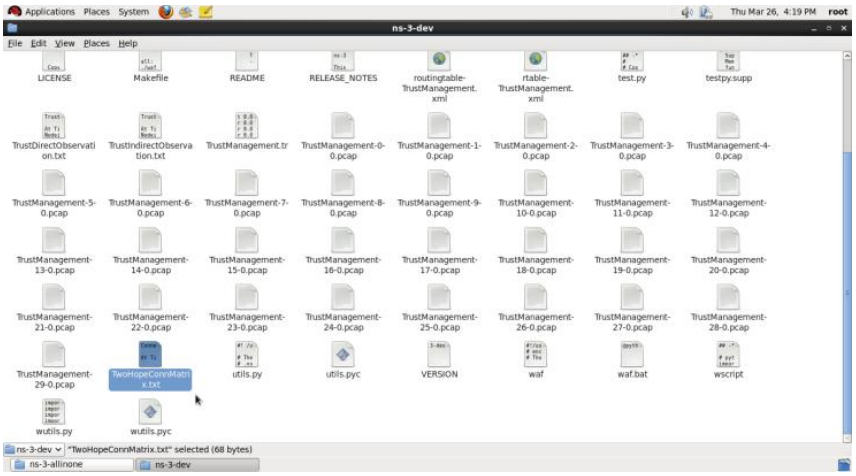

Figure 5 Two hop matrix is generated

- In Net Admin we can see animation using .xml file for simulation purpose

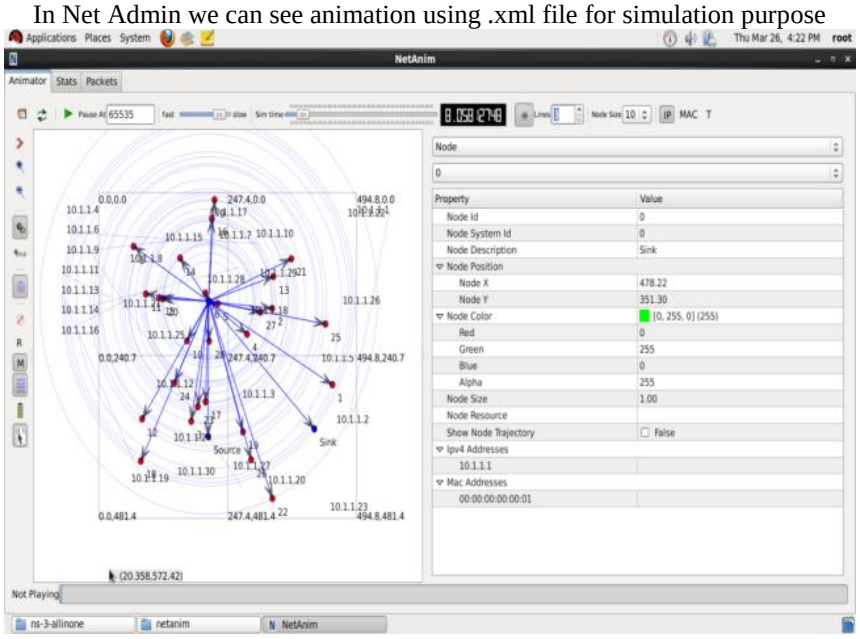

Figure 6 Net Admin showing animation

VII. CONCLUSION AND FUTURE WORK

A unified trust management security scheme is used to enhance the security of MANETs Using 'Uncertain Reasoning'. System evaluates the trust values of observed nodes in MANETs. Misbehavior such as 'Dropping' or 'Modifying packets', can be detected through trust values which is obtained by direct and indirect observation and nodes with low trust values will be excluded or remove by the routing algorithm. In this way secure routing path can be established in malicious environments which can help to improves throughput and packet delivery ratio.

REFERENCES

1. Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning", IEEE transaction paper 2014.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

2. Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani "A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE transaction paper 1999.
3. Q. Guan, F. R. Yu, S. Jiang and V. Leung, "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications," IEEE Trans. Veh. Tech., vol. 61, pp. 2674 –2685, July 2012.
4. Kejun Liu, Jing Deng, Pramod K. Varshney, Kashyap Balakrishnan, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" IEEE transaction paper 2011
5. Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," IEEE Trans. Dependable and Secure Computing, vol. 3, pp. 386–399, Oct.–Dec. 2006.
6. Bu, F. R. Yu, P. Liu, P. Manson, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks,"IEEE Trans. Veh. Tech., vol. 60, pp. 1025–1036, Mar. 2011.
7. S. Bu, F. R. Yu, X. P. Liu, and H. Tang, "Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks," IEEE Trans. Wireless Commun., vol. 10,pp. 3064 –3073, Sept. 2011.