ISSN 2278 - 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 01 - 05 (2015)
Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India
http://warse.org/IJATCSE/static/pdf/Issue/iceec2015sp01.pdf

Trust Assurance Mechanism against Gray Hole Attack in Mobile Ad Hoc Networks

Subi V S[1], Nishanth N[2]
[1]TKM College of Engineering, India, subivs1212@gmail.com
[21]TKM College of Engineering, India, nishtkm@gmail.com

e and black hole attacks are the major routing attacks in MANET (Moblie Ad hoc NETwork). In Gray hole attack the packets are dropped selectively by the attacker node after correctly participating in the route discovery phase. In this paper a trust algorithm based on uncertain reasoning is used for the gray hole attack detection. AODV (Ad-hoc On-demand distance Vector) is used as the routing protocol. Direct and indirect observations are used for the trust evaluation of a node. These observations along with packet drop checking mechanism provide more accurate trust value. Based on this value the behavior of each node is predicted and the attacker node is detected. The removal of the attacker node is done by flooding alarm packets in the network. Thereby trust of the participating nodes in the network is assured by a less complex trust assurance mechanism.

Key words: AODV, Gray hole attack, MANETs, Trust Management

INTRODUCTION

MANET is a self-configuring network of mobile nodes which communicate with each other in the absence of any centralized administration. These networks use wireless medium for communication. Since the use of bandwidth constrained wireless medium for the transmission of all the signals, they are more prone to physical security threats compared to landline networks. MANET is vulnerable to many types of attacks because of its characteristics like dynamic topology, node mobility, distributed cooperation and lack of centralized administration. MANETs are mostly suffered by black hole and gray hole attacks because these problems can be easily deployed in MANETs.

Routing has a major role in MANET. In most routing protocols, nodes exchange information about the topology of the network so that routes can be established between a source and a destination [1]. In MANET nodes are both routers and hosts. Two types of routing protocols were proposed for MANETs: proactive and reactive. Proactive routing protocol periodically transmits the control messages for updating the neighboring routes in the routing table. Reactive routing protocol are on-demand routing protocols which find the route to the destination only whenever the source wants to send the data. AODV [2], DSR and DSDV are the main reactive routing protocols.

Black hole and gray hole are the major routing attacks in MANET [3], [4]. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In flooding based protocol, if the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. This malicious node then can choose whether to drop the packets to perform a denial-of-service attack. Selective black-hole attack is known as gray-hole. In gray-hole attack, the malicious nodes participate correctly in route discovery process. But once a route is selected through them to reach destination, they will drop the data packets selectively. This is shown in Fig.1. As because only partial data packets are dropped, gray-hole attack is even harder to detect than black hole attack.

Trust based security systems are more suitable for MANETs. Even though several work [5], [6] has been carried out in this area, only few of them [6], [7] considered the secondhand information from neighboring nodes. More accurate trust value is obtained from both direct observation and indirect observation.

In this paper trust based gray-hole attack detection is proposed. It consists of trust algorithm which uses uncertain reasoning for the trust evaluation. Second hand information is considered in the indirect trust computation. Trust is assured by detecting and removing the malicious nodes from the network.

The remainder of this paper is organized as follows. Related work and the trust model and its two components are presented. It also depicts the Beta distribution and how to use it in trust evaluation from direct observation, the Dempster-Shafer theory and how to use it in the trust evaluation from indirect observation.

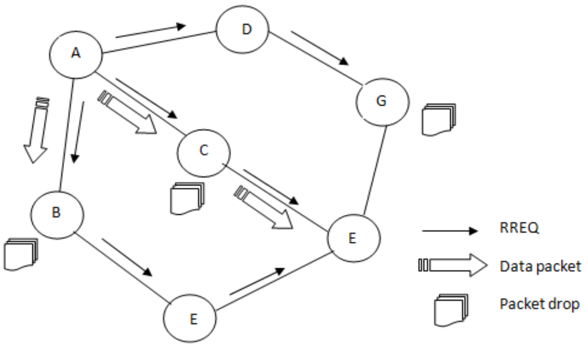

Fig 1: Gray-hole, black-hole and packet dropping attack in MANET. B-black hole attacker, C-gray hole attacker, D – packet dropping attacker.

Trust based gray hole attack detection, performance and effectiveness of the proposed scheme are presented in the following sections.

RELATED WORK

Prevention and detection of gray hole and black hole attack is a major issue in reactive routing protocols of MANET. In this paper trust based attack detection is proposed, it uses both direct observation and indirect observation. In [8] Kannan Govindan and Prasant Mohapatra presented a detailed report on various trust computing approaches that are geared towards MANETs. In this paper beta distribution is used for the trust value from direct observation. In [9] a beta reputation system is described and flexibility, simplicity and its foundation on statistics theory are the advantages of the beta distribution. Secondhand information from the neighboring nodes is combined using Dempster Shafer Theory (DST). DST combination rule is more suitable for combining the different trust value. In [7] the authors proposed a trust management scheme for mobile ad-hoc network using uncertain reasoning. In the proposed trust management scheme, the trust model has two components: trust from direct observation and trust from indirect observation. Trust from direct observation is derived using Bayesian inference which is a type of uncertain reasoning. In indirect observation the trust value is derived using the Dempster-Shafer theory which is another type of uncertain reasoning. Since Bayesian inference is used in the direct trust calculation full probability model should be defined. This is one of the demerits of the proposed scheme.

In [10] C. Zouridaki, B. L. Mark, M. Hejmo and R. K. Thomas proposed a trust establishment scheme for MANETs. Each node forms an opinion about each of the other nodes based on both first and second-hand observation data collected from the network. The opinion metric is incorporated into ad hoc routing protocols to achieve reliable packet delivery even when a portion of the network exhibits malicious behavior. But the proposed trust establishment scheme makes use of a Bayesian approach.

In [11] a Robust Cooperative Trust Establishment for MANETs is proposed. In the proposed scheme, each node determines the trustworthiness of the other nodes with respect to reliable packet forwarding by combining first-hand trust information obtained independently of other nodes and second-hand trust information obtained via recommendations from other nodes. First-hand trust information for neighbor nodes is obtained via direct observations at the MAC layer whereas first-hand information for non-neighbor nodes is obtained via feedback from acknowledgements sent in response to data packets. The proposed scheme exploits information sharing among nodes to accelerate the convergence of trust establishment procedures, yet is robust against the propagation of false trust information by malicious nodes.

Several schemes were proposed for black-hole and gray hole attack prevention and detection in MANET. In [12] a modified DSR routing protocol is proposed for the detection and removal of gray-hole attackers. It is a non-cryptographic technique. It uses IDS nodes for the gray-hole detection. The major limitations are the placement of IDS nodes, suspected node should be within the range of any one of the IDS nodes, if the IDS nodes do not cover the entire network, detection and isolation of gray-hole nodes may not be possible. In this paper AODV is used as a routing protocol. It is modified by including trust algorithm for the detection and removal of the gray hole attack. AODV protocol consists of three types of control packets, RREQ (route request), RREP (route reply) and route error packets. These packets are considered separately while calculating the trust value.

In [13] the authors proposed a co-operative black hole attack prevention method. This approach to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and is eliminated.

TRUST MODEL IN MANETS

A. Definition and Properties of Trust

With respect to the MANET sense trust can be defined in different ways. The trust of a particular node is a subjective assessment by an agent/other peer node on the reliability and accuracy of information received from or traversing through that node in a given context [8].

B. Trust Model

In this paper the trust is taken as a real number which ranges between 0 and 1.By definition, the trust value is the expectation of a subjective probability that a trustor uses to decide whether or not a trustee is reliable [7]. Trust value of a node is calculated both from direct and indirect observation. Beta distribution is used for the direct trust evaluation. Secondhand information from the neighboring nodes is combined using Dempster-Shafer Theory.

C. Trust Evaluation with Direct Observation

Initial trust is calculated using beta distribution [9]. Trust T is considered as a random variable taking values on the interval [0, 1] [7] and is assumed to follow a beta distribution. A realization of T is taken to be the trust value associated with the node. Since T is assumed to be beta distributed, trust is represented by the two parameters of the beta distribution. In this paper trust is defined as the expected value of the beta distribution. Expected value of beta distribution is given by

$$T = \alpha/(\alpha + \beta) \qquad (1)$$

Where α and β are the parameters of beta distribution. α is one more than the number of packets forwarded correctly and β is one more than the number of packets dropped by a node under observation.

At the initial stage there are no observations among the nodes in the network. Hence the value of and α and β are taken as 1. Then, at the subsequent levels α and β are calculated recursively as

$$\alpha_n = \alpha_{n-1} + x_{n-1} \qquad (2)$$

$$\beta_n = \beta_{n-1} + y_{n-1} - x_{n-1} \qquad (3)$$

Where x is the number of forwarded packets and y is the number of received packets.

D. Trust Evaluation with Indirect Observation

Dempster Shafer Theory is used for combining the opinion from the neighbouring nodes. Dempster-Shafer theory combines multiple neighbor nodes' belief on the condition that evidence from different neighbor nodes is independent [14]. For MANET environment the frame of discernment consist of three components.

Frame of discernment, Θ = {H, H', H∪H'}
H = Node is trustworthy
H' = Node is not trustworthy
H∪H'= Node is either trustworthy or untrustworthy
DST rule of combination is given by

$$m_1(A) = \frac{\sum_{X\cap Y=A} m_1(X)m_2(Y)}{1-\sum_{X\cap Y=\emptyset} m_1(X)m_2(Y)} \quad (4)$$

Where X, Y, A ε Θ and m(A) is the belief function for the observed node.

Let p be the probability that an observed node is trustworthy. The basic probability assignment by an observer node for a trusted observed node is given by

$$m_1(H) = p$$
$$m_1(H') = 0$$
$$m_1(H\cup H') = 1 - p \quad (5)$$

If the observed node is untrustworthy then the basic probability assignment becomes

$$m_1(H) = 0$$
$$m_1(H') = p$$
$$m_1(H\cup H') = 1 - p \quad (6)$$

GRAY-HOLE ATTACK DETECTION BASED ON TRUST

Network model is shown in Fig. 2. It consists of two gray-hole nodes and one black-hole node. All the nodes are mobile nodes. AODV is used as routing protocol. It has two main phases, route discovery and route maintenance. Whenever source S wants to transmit the data it initiates a RREQ packet and is received by all the neighboring nodes. Either the destination node D or any intermediate node which has a route to destination, reply with a RREP packet containing the source route. RREP packet is received by the source node. This completes the route discovery phase.

During the route discovery phase, each node overhears the traffic of its neighboring nodes and takes a measure of how many packets are received and out of this how many are forwarded.

AODV consist of route request packets, route replay packets, route error packets and data packets. For each type of packets separate measures were taken, then compute average value of beta distribution for each type of packets. Different weightings are given for each value. During the route discovery phase more weightage is given to route request packets, route replay packets and route error packets.

Trust obtained by the direct observation is

$$T_{dob} = w_1 t_{rq} + w_2 t_{rp} + w_3 t_{er} + w_4 t_d \quad (7)$$

Where $w_1+w_2+w_3+w_4=1$ and $0 \leq T_{dob} \leq 1$.
Where trust value based on route request packet

$$t_{rq} = \alpha_{rq} / (\alpha_{rq} + \beta_{rq}) \quad (8)$$

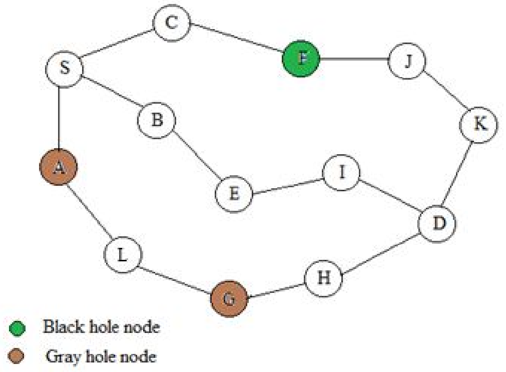

Fig 2: Network model

trust value based on route replay packet

$$t_{rp} = \alpha_{rp} / (\alpha_{rp} + \beta_{rp}) \quad (9)$$

trust value based on route error packet

$$t_{re} = \alpha_{re} / (\alpha_{re} + \beta_{re}) \quad (10)$$

trust value based on data packet

$$t_d = \alpha_d / (\alpha_d + \beta_d) \quad (11)$$

Packet dropping is checked using two methods. First one is using average difference. If

$$\frac{\alpha_{n-1}}{\alpha_{n-1}+\beta_{n-1}} - \frac{\alpha_n}{\alpha_n+\beta_n} \geq H_1 \quad (12)$$

Then trust from direct observation, T_{dob} is reduced to T_{dob} / γ, γ is a constant. Otherwise T_{dob} remains as the same. Second one is using the ratio of number of forwarded packets to number of received packets. If the ratio is less than the assigned threshold value trust value is deducted by a constant value.

Then the direct trust value is obtained using the equation (13).

$$T_a(b) = \boldsymbol{\lambda}\, T_{dob} + (1-\boldsymbol{\lambda})\, T_{pe} \quad (13)$$

Where T_{pe} is the trust value of the observed node from past experience.

After the aggregation of trust recommendations, total trust of node D is calculated as

$$T_A(D) = \sigma T_D(D) + (1-\sigma)\, R_A(D) \quad (14)$$

σ is the waitage given to the direct observation. At the initial stage there are no observations. Hence $\alpha_0 = \beta_0 = 1$. Hence initial trust level is equal to 0.5 for all nodes. During the packet transmission; each node updates the trust value using the trust algorithm.

Whenever the trust value is below the threshold value the observer node flood the network with alarm packets and thereby isolate the malicious node from the network.

Trust Algorithm

```
Compute the trust from direct observation using (1)
Check for packet drop
 if long term average- current average is greater than the threshold value then
      decrease the trust value
  else
      if the ratio of number of forwarded packets to number of received packets is greater than the threshold value then
          trust value is deducted by a constant value.
      end if
  end if
 Calculate total direct trust by combining direct trust with trust from past experience from (13).
Combine the recommendations from each neighboring node using DST rule from (4).
Calculate the total trust from (14).
```

SIMULATION RESULTS AND DISCUSSIONS

The proposed scheme is implemented using ns2. The parameters used in the simulation are given in the table 1.

In the simulation the effectiveness of the paper is evaluated in an insecure MANET environment. Three different scenarios were considered, a network without any attack, with gray hole node, and with the proposed scheme. There are three performance metrics are used in the performance evaluation: 1) Throughput is the amount of data moved successfully from one place to another in a given time period. From Fig. 3, throughput is increased by the use of proposed scheme; 2) Packet delivery ratio is the ratio of the number of delivered data packet to the destination. As in the Fig.4, with increase in number of nodes in the network PDR decreases because congestion in the network increases so packets are dropped due to the collisions.;3)Normalized Routing Load (or Normalized Routing Overhead) is defined as the total number of routing packet transmitted per data packet. It is calculated by dividing the total number of routing packets sent (includes forwarded routing packets as well) by the total number of data packets received. It is slightly higher compared to the environment without attack which is shown in Fig 5.

Table 1: Simulation Parameters

Parameter	Value
Application protocol	CBR
CBR transmission time	1s to 100s
CBR transmission interval	0.5s
Packet size	512 bytes
Transport protocol	UDP
Network protocol	IPv4
Routing protocol	AODV
Data rate	2Mbps
Propagation pathloss model	Two-ray
Simulation area	1000m x 1000m
Number of nodes	10, 15, 20, 25, 30, 40, 50, 60
Simulation time	150s

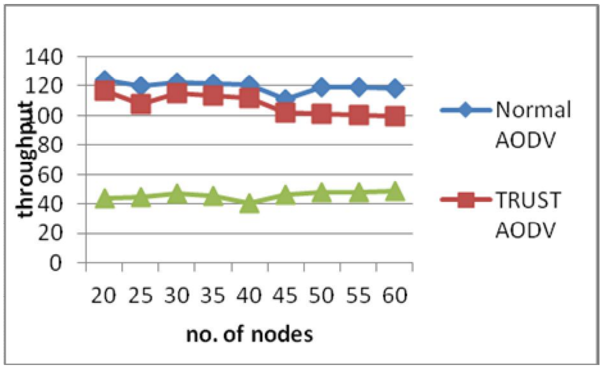

Fig 3: Throughput versus the number of nodes in the network.

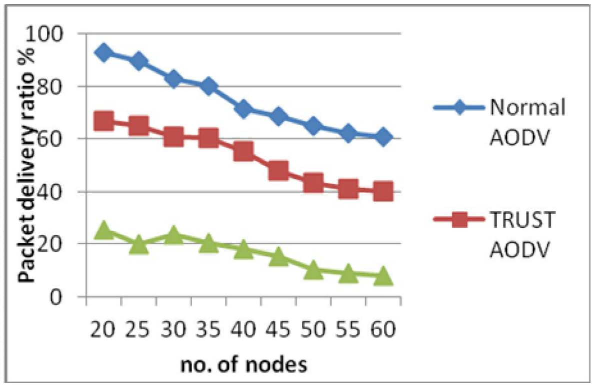

Fig 4: Packet delivery ratio (PDR) versus the number of nodes in the network.

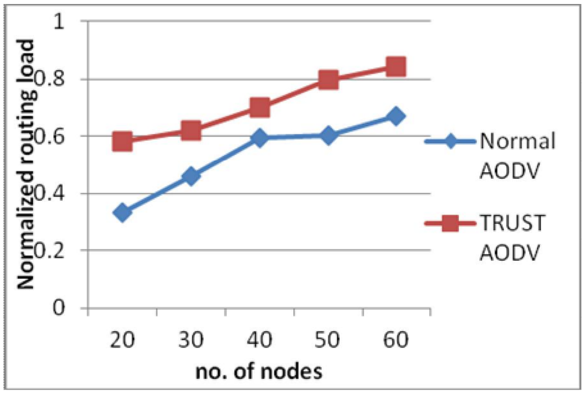

Fig 5: Routing load versus the number of nodes in the network.

CONCLUSION

In this paper, a trust algorithm based on uncertain reasoning for the gray hole attack detection in MANET is proposed. Beta distribution and Dempster-Shafer theory are used for the evaluation of trust value of observed nodes in MANET. Trust is assured by detecting and removing the malicious nodes from the network with AODV (Ad-hoc On-demand distance Vector) as the routing protocol. Gray hole attack and black hole attacks are detected using the trust value calculated from both direct and indirect observations. The results of MANET routing scenario positively support the scheme which improves packet delivery ratio and throughput in a malicious environment considerably, with slightly increased normalized routing load. The removal of the attacker node is done by flooding alarm packets in the network.

REFERENCES

[1] Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Networks” IEEE Communications Magazine, October 2002 pp.70-75.

[2] C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc on-demand distance vector (AODV) routing,” IETF RFC 3561, Jul. 2003.

[3] Soufiene Djahel, Farid Na¨ıt-abdesselam, and Zonghua Zhang “Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges” IEEE communications surveys & tutorials, vol. 13, no. 4, fourth quarter 2011.

[4] Rajesh kumar.g and dr.k.r.valluvan “performance evaluation of dynamic source Routing under black hole attack” Journal of Theoretical and Applied Information Technology 10th August 2014. Vol. 66 No.1.

[5] P. Albers et al., “Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches,” 1st Int’l. Wksp. WL Info. Sys., 4th Int’l. Conf. Enterprise Info. Sys., 2002.

[6] Xiaoqi Li, Lyu, M.R. Jiangchuan Liu “A Trust Model Based Routing Protocol for Secure Ad Hoc Networks” IEEE Proceedings pg no. 1286 - 1295 Vol.2,2004.

[7] 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 Transactions on Vehicular Technology, 2013

[8] Kannan Govindan, Prasant Mohapatra,”Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey”, IEEE Communications Surveys & Tutorials, Vol. 14, No. 2, Second Quarter 2012

[9] Audun Jøsang and Roslan Ismail “The Beta Reputation System”, 15th Bled Electronic Commerce Conference, June 17 - 19, 2002.

[10] C. Zouridaki, B. L. Mark, M. Hejmo ,R.K. Thomas A Quantitative Trust Establishment Framework for Reliable Data Packet Delivery in MANETs, November 2005.

[11] Charikleia Zouridaki, Brian L. Mark, Marek Hejmo and Roshan K. Thomas_ “Robust Cooperative Trust Establishment for MANETs”, October , 2006.

[12] M. Mohanapriya and Ilango Krishnamurthi “Modified DSR protocol for detection and removal of selective black hole attack in MANET”, Computers and Electrical Engineering 40 (2014) 530–538.

[13] Latha Tamilselvan “Prevention of Co-operative Black Hole Attack in manet journal of networks”, vol. 3, no. 5, may 2008.

[14] Thomas M. Chen and Varadharajan Venkataramanan “Dempster-Shafer Theory for Intrusion Detection in Ad Hoc Networks”. IEEE internet computing, december 2005.