ISSN 2278 – 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 16 - 21 (2015)
Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India
http://warse.org/IJATCSE/static/pdf/Issue/iceec2015sp04.pdf

Secure Routing in Mobile Ad-hoc Networks Using Evidence Theory

Shyma M[1], Nishanth N[2]
[1]Student T.K.M College of Engineering, India, shymaprasad89@gmail.com
[2]Professor T.K.M College of Engineering, India, nishtkm@gmail.com

Abstract*:* In Mobile Ad-hoc NETworks (MANETs) nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The open medium and wide distribution of nodes or the lack of centralized infrastructure make MANET vulnerable to malicious attackers. Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Hence providing secure route is the most challenging task to be carried out in MANET environment. This work proposes a unified trust management scheme for MANETs to provide secure routing. In this scheme every node calculates the trust value of its one hop neighbor by both direct observation and recommendations provided by other neighbors. The calculated trust values are then used for calculating the path trust of all possible paths between any source and destination node by AODV routing protocol which may calculate shortest path in the absence of trust incorporation. From these, shortest trusted path is selected for communication.

Key words: MANETs; Security; Trust; Trust management.

INTRODUCTION

Mobile Ad hoc Networks (MANETs) [1] represent complex distributed systems that consist of wireless nodes that can dynamically and freely self-organize into arbitrary and temporary ad hoc network topology. This allows people and devices to seamlessly inter networked in areas where no pre-existing communication infrastructure exist. In MANET a primary requirement for the establishment of communication among nodes is that nodes should cooperate with each other. In the presence of malicious nodes, this requirement may lead to serious security concern. Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in MANET [2].The unique characteristics of MANETs such as dynamic topology and resource constrained devices pose a number of nontrivial challenges for efficient and secure routing protocols [3], [4]. Therefore, establishing and quantifying behavior of nodes in the form of trust is essential for ensuring proper operation of MANET.

Most of the routing protocols developed for MANETs, such as DSR, AODV and DSDV are based on the multi hop assumption and they do not incorporate any security mechanism [5]. To increase MANET performance to enforce cooperation in the network reputation and trust based schemes have been developed. This scheme utilizes the past behavior of end-users to enable a node to decide whether other nodes are cooperative and trustworthy [6]. In this paper, our scheme is a security mechanism that mainly protects AODV against two types of misbehavior, dropping packets and modifying packets. That is, this scheme is a trust based secure routing for MANET using evidence theory [7], [8]. As compared to the trusted AODV protocol this work will use both direct observation and recommendations for trust computation. The traditional AODV only finds minimum hop path, where as this scheme consider the number of hops from source to destination as well as the path trust from source to destination and finds highly trusted shortest path for communication.

The latest work in this field also considers both direct and indirect observation for trust calculation [9]. This work is as an enhancement to the existing work, by eliminating the vulnerabilities of it. This trust management scheme provides some modifications in both direct and indirect trust calculations. The added advantage of this paper is that trust satisfaction factor and penalty factor are considered in the direct trust calculation to give penalty to misbehavior. In the calculation of Bayesian trust value a penalty factor is considered to give more weights on misbehavior, and to reduce the trust value of a node when it misbehaves. With indirect observation from neighbor nodes of the observer node, the trust value is derived using either Dempster-Shafer theory (DST) or Murphy's rule of combination [10], [11]. The advantage of this scheme is that, it will eliminate the conflict of using DST. The DST rule becomes inaccurate when the conflict becomes high. For such situation Murphy's rule is used as an alternative rule for combining the evidences from various observers. Then over all trust value between observer and observed node is calculated as the weighted sum of trust value obtained from direct observation and trust value obtained from recommendations. Then these calculated trust values are incorporated with the AODV routing protocol to provide secure routing. The path trust is calculated as the sum of trust values between all pair of nodes between source and destination. Then the secure routing protocol will select highly trusted shortest path.

RELATED WORKS

In MANETs, an untrustworthy node can create considerable damage and adversely affect the quality and reliability of data. Computing the trust level of a node has a positive influence on the confidence with which an entity conducts transaction with that node. Trust based security

ISSN 2278 – 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 16 - 21 (2015)
Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India
http://warse.org/IJATCSE/static/pdf/Issue/iceec2015sp04.pdf

schemes are studied recently in [12], [13]. Trust computations consist of three components: 'experience', 'recommendation', 'knowledge'. The 'experience' component of trust for each node is directly measured by their immediate neighbors and kept updated at regular intervals in the trust table. The existing trust table is propagated to all other nodes as 'recommendation' part of trust. At a regular interval, the previously evaluated trust is included in the current 'knowledge' component of total trust.

An Ad-hoc on-demand trusted path distance vector (AOTDV) is proposed for MANETs [14]. It is a trust based multi path routing using AODV protocol. AOTDV adopts a hop-by-hop routing mechanism in which the source is not expected to know which neighbor is the next hop. In this scheme a source establishes multiple trustworthy paths as candidates to a destination in single route discovery. The main problem of this method is that it considers only direct observation for trust computation. Hence the chance of detecting attacker node that acts genuine to some nodes and malicious to some other nodes will be very less. Hence this scheme is not suitable for MANETs having Gray hole [selective black hole] attackers.

The authors of [15] use Bayesian inference to evaluate the direct trust and Dempster-Shafer theory (DST) to evaluate indirect trust. Dempster's rule for combination is a procedure for combining independent pieces of evidence. The major drawback of this method is that when the conflict between the observers is high the DST rule of combination becomes inaccurate. That is at high conflict conditions, using DST as trust combination rule will gives false alarm. So the recommendation trust value using DST is incorrect or inaccurate.

TRUST COMPUTATION

A. Network Model

In the network model a number of nodes are placed randomly in the simulation area as shown in Fig: 1. There are two types of nodes in the network, normal nodes which follow the routing rules and compromised node which drop or modify the packets maliciously. The number of malicious nodes is minor compared to the total number of nodes in the network. In the network one node is set as source node and another one is set as destination. It is required to calculate a trusted minimum hop path from source to destination node. The malicious node in the path from source to destination will claim that it is having a shortest route to the destination. So the source node will always select the route through malicious node for its communication with the destination. Hence the data packets send by the source node will never reaches the destination. For secure communication malicious nodes have to be detected eliminated from the communication path. And another shortest path that does not contain malicious node as a router has to be selected for communication. For this a trust based secure routing scheme is proposed.

B. Trust model

Trust is interpreted as the degree of belief that a node in the network will carry out a task that it should. Trust can also be defined as the expectation of a subjective probability that a

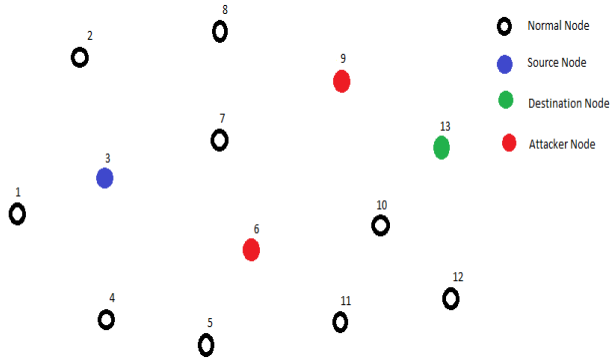

Fig: 1 Mobile ad hoc network model

truster uses to decide whether or not a trustee is reliable. Based on the definition and properties of trust in MANETs, the proposed scheme evaluates trust by a real number T, with a continuous value between 0 and 1. In this scheme initially every node calculates the direct trust of each of its one hop neighbors periodically and keeps updating its routing table. This is done by observing the packet forwarding behavior of them. Then they calculate the indirect observation trust from the recommendations provided by other one hop neighbors [16].

Combining the trust value, from direct observation and the trust value from recommendations, we can get a more realistic and accurate trust value of a node in MANETs. Then the overall trust value can be calculated as the weighted sum of direct trust and recommendation trust as

$$T = W_1 * T^D + W_2 * T^R \quad (1)$$

Where W_1 and W_2 are the weight assigned to direct observation trust and recommendation trust respectively, $W_{1+}W_2=1$. And T^D is the trust value obtained from direct observation, T^R is the trust value obtained from recommendation. Then the trust value between pair of nodes is used to calculate the path trust. In this network model there are several possible paths between source and destination node with different hops. The best routing algorithm will select a route that is having higher path trust value and minimum hop count. The routing protocol will first calculate path trust value for all possible paths and then select a highly trusted minimum hop path from these available paths.

C. Trust Computation of One-hop Neighbors

In the direct observation, it is assumed 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. In this proposed scheme direct observation trust is computed as the

ISSN 2278 – 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 16 - 21 (2015)
Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India
http://warse.org/IJATCSE/static/pdf/Issue/iceec2015sp04.pdf

product of two components (in Algorithm 1), the first component of direct observation trust is calculated by observer node using Bayesian inference [17]. This component is termed Bayesian trust. And the second component is trust satisfaction factor [18]. At the beginning when there is no observation history available, then the trust value of a node is taken as 0.5. That means the node is seemed as neutral when no history records behaviors is established. The value trust can be revised continuously through follow-up observation. Then trust from Bayesian inference is taken as the expectation of beta distribution along with a penalty factor to give more weight on misbehavior. Incorporating penalty factor can help the proposed scheme distinguish the malicious node quickly and avoid them disrupting the normal traffic between benign nodes again because of two reasons. Firstly, this can lower the trust of an attacker when it misbehaves. Secondly, the trust of the attack will not recover quickly even if it forwards a large number of packets correctly due to the impact of the penalty factor. The penalty factor is inspired by our daily lives in human society, where a scandal can badly affect a person who has a good reputation. What's more, it is hard to quickly recover a good reputation. The factor of punishment makes the trust evaluation more realistic. Algorithm 1 will describes the trust computation with direct observation. For any source node set variable for the number packets generated by it and for the number of packets forwarded correctly by each of its neighbors.

Algorithm 1 Trust Calculation with Direct Observation

1: **if** node i, which is an observer, finds a one hop neighbor, **then**
2: set variables, total packets generated, no. of packets forwarded
3: **if** node i, finds that its 1 hop neighbor, receives a packet, **then**
4: the total packets generated increases one
5: **if** node i, finds that its 1 hop neighbor, forward the packet successfully, **then**
6: the no. of packets forwarded increases one
7: **end if**
8: **end if**
9: **end if**
10: Calculates the Bayesian trust B_T, from (2)
11: Calculates Trust satisfaction factor T_S, from (3)
12: Calculates the Direct observation trust T^D, from (4)

Algorithm 2 Trust Calculation with Recommendation

1: **if** node i, which is an observer, finds no one hop neighbor, **then**
2: set recommended trust to zero
3: **else**
4: **if** node i, finds only a single neighbor, **then**
5: set recommended trust as the direct trust of 1 hop neighbor
6: **else**
7: **if** node i, finds more than one neighbor, **then**
8: Calculates conflict factor C, compare with threshold, **then**
9: Calculate recommended trust T^R, from (5)
10: **end if**
11: **end if**
12: **end if**

Table I: Simulation Parameters

Parameter	Value
Application protocol	CBR
CBR transmission time	1s to 500s
CBR transmission interval	0.5s
Packet size	512 bytes
Transport protocol	UDP
Network protocol	IPv4
Routing protocol	AODV
MAC protocol	IEEE 802.11
Physical protocol	IEEE 802.11b
Data rate	2Mbps
Transmission power	6dBm
Radio range	180m
Propagation path loss model	Two-ray
Simulation area	500X500, 1000X1000
Number of nodes	10,20,30,40,50,60
Simulation time	600s

Y_{n-1}- Number of packets generated by a node

X_{n-1}-Number of packets forwarded correctly by its neighbor

Z_{n-1}- Number of failed packets

$Z_{n-1}=Y_{n-1}-X_{n-1}$

Let, $\alpha_0=\beta_0=1$

$\alpha_n=\alpha_{n-1}+X_{n-1}$

$\beta_n=\beta_{n-1}+Y_{n-1}-X_{n-1}$

Then the Bayesian trust can be calculated as

$$B_T = \frac{\alpha_n}{\alpha_n+\gamma\beta_n} \quad (2)$$

Where

$$\gamma = \begin{bmatrix} 2 & if\ Z_{n-1} > X_{n-1}\ and\ Z_{n-1}-X_{n-1} < \frac{1}{2}(Y_{n-1}) \\ 4 & if\ Z_{n-1} > X_{n-1} and\ Z_{n-1}-X_{n-1} \geq \frac{1}{2}(Y_{n-1}) \\ 1 & else \end{bmatrix}$$

The trust satisfaction factor

$$Ts = \frac{X_{n-1}+1}{Y_{n-1}+2} \quad (3)$$

Then the direct observation trust of Node B by Node A is calculated as the product of Bayesian trust and trust satisfaction factor. The trust satisfaction factor will lower the trust value when the failure rate is high, but it doesn't lower

ISSN 2278 – 3091

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 16 - 21 (2015)
Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India
http://warse.org/IJATCSE/static/pdf/Issue/iceec2015sp04.pdf

the trust even though the node will forward a large number of packets correctly. Then the direct observation trust T^D is

$$T^D = B_T * T_S \quad (4)$$

For any source node set variable for the number packets generated by it and for the number of packets forwarded correctly by each of its neighbors.

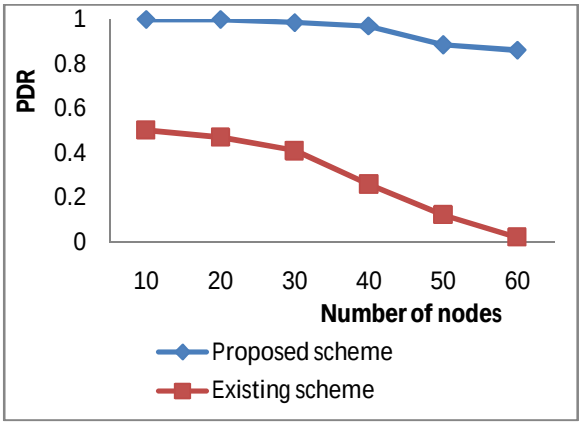

Fig 2: PDR v/s Number of node

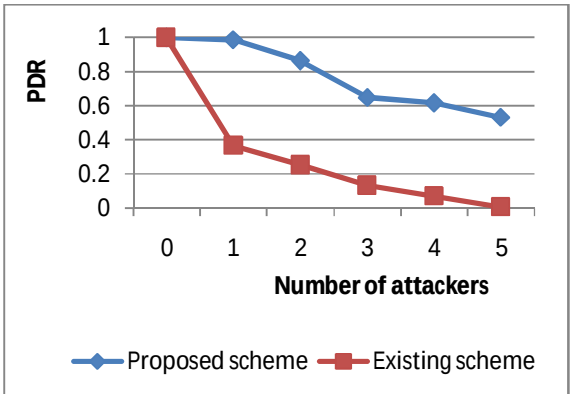

Fig 3: PDR v/s Number of Attackers

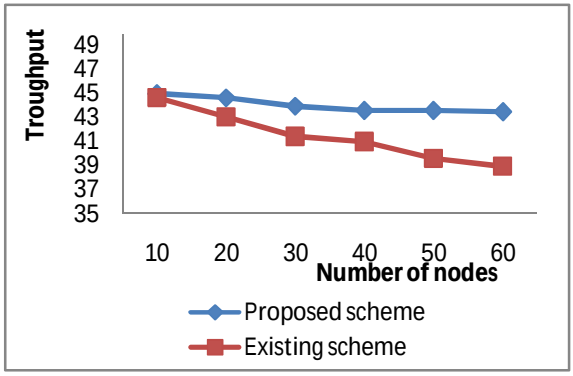

Fig 4: Throughput v/s Number of nodes

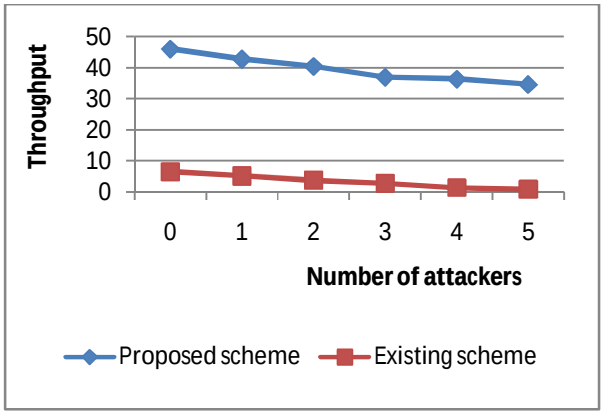

Fig 5: Throughput v/s Number of Attacker

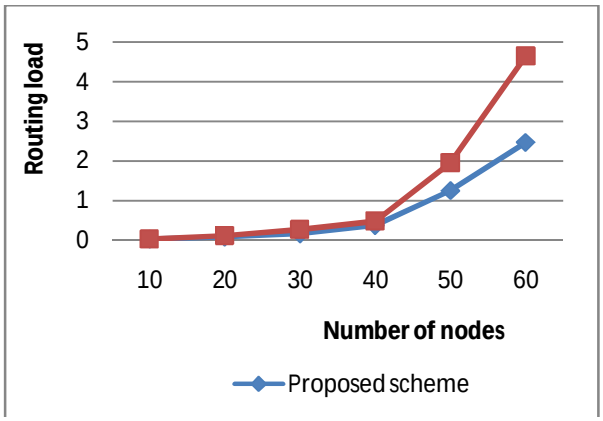

Fig 6: Routing load v/s Number of nodes

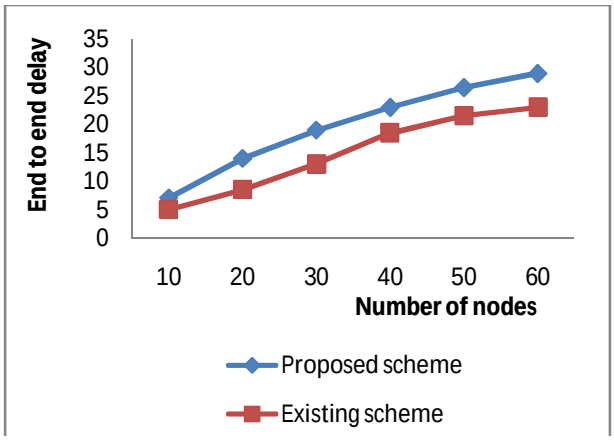

Fig 7: End to end delay v/s Number of nodes

A. *Indirect Trust Computation*

The recommendations provided by neighbor nodes are used to evaluate the trust value of the observed node. That is every node is calculating the indirect observation trust of its 1 hop neighbors from the recommendations provided by other 1 hop neighbors (in Algorithm 2). If there is no one hop neighbor to provide recommendations then the indirect

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 16 - 21 (2015)
Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India
http://warse.org/IJATCSE/static/pdf/Issue/iceec2015sp04.pdf

observation trust is taken as zero. And if there is only single neighbor to provide recommendations then indirect observation trust is taken as the direct observation trust of recommender by the observer. If there is more than one recommendation provided by one hop neighbors then some combining methods are used to find out the overall trust value. For combining these recommendations either DST or Murphy rule of combination is used, based on the value of conflict factor C [19], [20].

In the indirect trust calculation first conflict factor is calculated. Based on the value of conflict either DST or Murphy rule is selected for indirect trust calculation. DST is the best method for trust computation at low conflict values. When the conflict becomes high then conflicts between different pieces of evidence are mismanaged by DST. The application of DST leads to an undefined condition and cannot be applied for trust computation.

Hence under high conflict condition Murphy rule is applied. The conflict factor C is the mass allocated to the empty set and is calculated as,

$$C = 1 - m(\phi) = 1 - [M_1(H)M_2(\bar{H}) + M_1(\bar{H})M_2(H)] \quad (5)$$

Then the indirect observation trust T^R is calculated as,

$$T^R = \begin{matrix} T^{DST} & for\ C \geq 0.25 \\ T^M & for\ C < 0.25 \end{matrix} \quad (6)$$

Where,

$$T^{DST} = M_{j1}(H) \oplus M_{j2}(H),\ T^M = \frac{1}{2}[M_{j1}(H) + M_{j2}(H)] \quad (7)$$

is the trust value obtained from Dempster's rule and the trust value calculated by Murphy's rule respectively.

E. Trust Based Secure Routing

Compared to the existing AODV scheme that uses the shortest path based on hop count, thrust based routing scheme derive the best routing path considering both trust values and hop count. The Dijkstra' algorithm is used to calculate the best routing path. Since minimization is used in the Dijkstra' algorithm (e.g., to find the shortest path with the minimal hop count in traditional AODV), it is need to convert the trust value to untrustworthy value. Then, we can minimize the untrustworthy value of a path using the Dijkstra' algorithm.

To this end, define the untrustworthy value between node 1 and node 2 as U_{12}, which can be calculated as U_{12}=1-T_{12}. The sum of untrustworthy values of a path is

$$U_{path} = \sum_{i=1}^{n-1} U_{ki\,ki+1} = \sum_{i=1}^{n-1}(1 - T_{ki\,ki+1}) \quad (5)$$

Where $T_{ki\,ki+1}$is the trust value between node ki and its one hop neighbor, node ki+1. Nodes k1, k2, . . . , kn belongs to the path with n − 1 hops. The best routing path satisfies the minimum of U_{path}.

SIMULATION RESULTS AND PERFOMANCE IMPROVEMENT

The proposed scheme is simulated in NS2 simulator with AODV routing protocol. The effectiveness of the scheme is evaluated in malicious environment. We compare the performance of the proposed scheme with that of AODV without security mechanism.

A. Simulation Environment Settings

We randomly placed nodes in the defined area. Simulations are performed in different scenario; with each scenario has a pair of nodes as the source and destination. The traffic used for simulation is constant bit rate traffic (CBR). The simulation parameters are listed in Table: I. In the simulation it is assumed that there are two types of nodes in the network, normal node and malicious node. Normal nodes are nodes that follow routing rules, where as malicious nodes will drop or modify packets maliciously. As compared to the total number of packets the number of malicious nodes is very less. In this adversary mode, proposed scheme is evaluated and compared with the original AODV protocol. We have simulated the networks with different numbers of nodes. Fig 2 is an example of the network set up, where node 3 is the source node, node 13 is the destination node and nodes 6 and 9 are malicious nodes. For node mobility, the random waypoint mobility model is adopted in 60 node MANET. The maximum velocity of each node is 0 to 20 m/s. Four performance metrics are considered for understanding the performance variation of MANET with and without malicious nodes. 1) Packet delivery ratio (PDR) is the ratio of the number of data packets received by a destination node to the number of data packets generated by the source node. 2) Throughput is the total size of data packets correctly received by a destination node every second. 3) Routing load is the ratio of number of control packets transmitted by nodes to the number of data packets received successfully by destination during the simulation. 4) Average end to end delay. It is the mean of end to end delay between a source node and a destination node with CBR traffic.

B. Performance Improvement

The original AODV and our scheme are evaluated in the simulation, where some nodes act maliciously by dropping or modifying packets. In Fig: 2 we compare PDR for AODV MANET with and without trust scheme, which includes nodes from 10 to 60. From the figure, we can see that the AODV MANET with trust has higher PDR as compared to original AODV. This is because the original AODV protocol does not have any security measurements, and the chance of dropping packets by malicious nodes is high. Hence the PDR is very low in the case of original AODV protocol. Where as in the proposed scheme the trust scheme will detect malicious nodes and hence the chance of reaching packets at the destination is high. So the Packet Delivery Ratio is also very high. We can also find that the PDR of both the schemes decreases gradually when the number of nodes grows. For small number of nodes the PDR high. As the number of nodes increases the packet drop increases. This is because the collision of sending messages becomes more frequent as the

International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 4 , No.4 Pages : 16 - 21 (2015)
Special Issue of ICEEC 2015 - Held on August 24, 2015 in The Dunes, Cochin, India
http://warse.org/IJATCSE/static/pdf/Issue/iceec2015sp04.pdf

number of nodes increases in the MANET. The PDR decreases even more as the number of attacker increases as in Fig: 3, this is because the black hole attacker will drop the packets without forwarding it to the receiver. Hence as the number of attacker increases number of dropped packets also increases drastically, that will reduce the PDR.

As compared to the existing scheme throughput of the proposed scheme is very high. This is because the security mechanism in the proposed scheme will increase the number of correctly received packets. It is observed from Fig: 4 that the throughput also decreases with number of nodes; this is because the number of packets received correctly decreases as long as the number of nodes increases. Fig: 5 reveal that the number of attackers has significant impact on the throughput of the network. As the number of attackers increases the throughput also decreases to a very low value. In Fig: 6, the result demonstrates that proposed scheme has a lower routing load. This is due to the fact that the security mechanism imposed by the proposed scheme will increase the number of packets correctly received by the destination.

The cost of adding security mechanism is increase in average end to end delay as compared to original AODV protocol. Fig: 7 show that the proposed scheme has a slightly higher average end-to-end delay than the existing scheme. This is because the trust computation and update time are added along with route discovery time of original AODV protocol. Also the trusted path is always a longer one as compared to the path provided by the original routing protocol. There is a trivial delay introduced by this scheme as compared to the existing scheme, but high security is guaranteed.

CONCLUSIONS

Owing to multi hop routing and absence of centralized administration in open environment MANETs are vulnerable to various security attacks. Hence providing secure route is the most challenging task to be carried out in MANET environment. This paper proposes a trust management scheme for MANETs to provide secure routing. In this scheme every node calculates the trust value of its one hop neighbor by both direct observation and recommendations provided by other neighbors that is indirect trust. We use packet forwarding ratio to evaluate the one hop neighbor trust. The calculated trust values are then used for calculating the path trust of all possible paths between any source and destination node by the routing scheme. AODV routing protocol may calculate shortest path in the absence of trust incorporation. By incorporating trust the AODV protocol will select shortest trusted path for communication. Dijkstra's algorithm normally used for calculating shortest path between any pair of nodes can be used for trusted path computation.

ACKNOWLEDGEMENT

The opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the Department of Justice.

The authors are thankful to Dr. S. Suresh Babu and the staff at Networking Laboratory, were the simulation works are performed.

REFERENCES

[1] J. Loo, J. Lloret, and J. H. Ortiz, *Mobile Ad Hoc Networks: Current Status and Future Trends*. Boca Raton, FL, USA: CRC, 2011.
[2] F. R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and Quality of Service (QoS) co design in cooperative mobile ad hoc networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2013, pp. 188–190, Jul. 2013.
[3] S. Marti, T. Giuli, K. Lai, and M. Maker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. ACM MobiCom*, Aug. 2000, pp. 255–265.
[4] W. Lou, W. Liu, Y. Zhang, and Y. Fang, "SPREAD: Improving network security by multipath routing in mobile ad hoc networks," *ACM Wireless Netw.*, vol. 15, no. 3, pp. 279–294, Apr. 2009.
[5] Asad Amir Pirzada, Chris McDonald, and Amitava Datta, "Performance Comparison of Trust-Based Reactive Routing Protocols," *IEEE Trans. Mob. Computing.*, VOL. 5, NO. 6, JUNE 2006
[6] C. Perkins, E. Belding-Royer, and S. Das, Ad hoc On-Demand Distance Vector (AODV) routing, Jul. 2003, *IETF RFC* 3561.
[7] S. 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. Technol.*, vol. 60, no. 3, pp. 1025–1036, Mar. 2011.
[8] Lef`evre E., Colot O., Vannoorenberghe P., Belief functions combination and conflict management, *Information Fusion Journal, Elsevier Publisher*, Vol. 3, No. 2, pp. 149-162, 2002.
[9] 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 Trans. Veh. Tech.*, 2014.
[10] T. M. Chen and V. Venkataramanan, "Dempster–Shafer theory for intrusion detection in ad hoc networks," *IEEE Internet Comput.*, vol. 9, no. 6, pp. 35–41, Nov./Dec. 2005.
[11] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey on trust and reputation management systems in wireless communications," *Proc. IEEE*, vol. 98, no. 10, pp. 1755–1772, Oct. 2010.
[12] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantitative trust establishment framework for reliable data packet delivery in MANETs," in *Proc. 3rd ACM Workshop SASN*, Nov. 2005, pp. 1–10.
[13] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor fusion using Dempster–Shafer theory," in *Proc. IEEE Instrumen. Meas. Technol. Conf.*, May 2002, pp. 7–12.
[14] N. Marchang, R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks," *IET Inf. Sec.*, Vol. 6, lss. 2,pp. 77-83 May 2011.
[15] T. M. Chen and V. Venkataramanan, "Dempster–Shafer theory for intrusion detection in ad hoc networks," *IEEE Internet Comput.*, vol. 9, no. 6, pp. 35–41, Nov./Dec. 2005.
[16] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey on trust and reputation management systems in wireless communications," *Proc. IEEE*, vol. 98, no. 10, pp. 1755–1772, Oct. 2010.
[17] Audun Josang, Roslan Ismail, "The Beta reputation system," *15th Bled Electronic Commerce Conf.*, 2002.
[18] K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, V. C. M. Leung, "A context-aware trust-based information dissemination framework for Vehicular networks," Internet of Things Journal, *IEEE* vol.2, pp. 121-132, 2013.
[19] Voorbraak F., On the justification of Dempster's rule of combination, Artificial Intelligence, 48, pp. 171-197, 1991.
[20] Murphy C.K., Combining belief functions when evidence conflicts, Decision Support Systems, *Elsevier Publisher*, vol. 29, pp. 1-9, 2000.