International Journal of Electrical and Electronics Research ISSN 2348-6988 (online)
Vol. 3, Issue 1, pp: (354-365), Month: January - March 2015, Available at: www.researchpublish.com

An Unified Trust Management Scheme for Enhancement of Security In MANETs

[1]Bharathchandar, M., [2]Vigneshwaran, S., [3]Vishal, R., [4]Vishalraj, M., [5]Mrs. Nithya, D

B.E, ECE department, Panimalar Engineering College, Chennai, india

***Abstract*: With recent advances in wireless technologies and mobile devices, mobile ad hoc networks (MANETs) have become popular as a key communication technology in military tactical environments. The distinctive features of MANETs such as open wireless transmission medium, nomadic and distributed nature make it vulnerable to many security attacks. In this paper we propose a unified trust management scheme that enhances the security in MANETs. In the proposed trust management scheme, the trust model has two components: trust from direct observation and trust from indirect observation. With direct observation, the trust value of an observed node is derived directly by the observer node based on the opinion of observer node alone . On the other hand, with indirect observation, also called second hand information, the trust value of an observed node is obtained from neighbour nodes of the observer node. Combining these two components in the trust model, we can obtain more accurate trust values of the observed nodes in MANETs. We then evaluate our scheme under the scenario of MANET routing. Extensive simulation results show the effectiveness of the proposed scheme. Specifically, throughput and packet delivery ratio can be improved significantly with slightly increased average end-to-end delay and overhead of messages.**

Keywords: **MANETs, Security, Trust Management, Uncertain Reasoning.**

I. INTRODUCTION

Mobile Ad hoc Networks (MANETs) have become popular as a key communication technology in military tactical environments such as establishment of communication networks used to coordinate military deployment among the soldiers, vehicles, and operational command centers [1],[2],[3]. There are many risks in military environments needed to be considered seriously due to the distinctive features of MANETs, including open wireless transmission medium, nomadic and distributed nature, lack of centralized infrastructure of security protection [4]-[6]. Therefore, security in tactical MANETs is a challenging research topic.

There are two complementary classes of approaches that can safeguard tactical MANETs:[8] *Prevention-based* and *detection-based* approaches. One issue of these prevention-based approaches is that a centralized key management infrastructure is needed,[9]-[12] which may not be realistic in distributed networks such as MANETs. In addition, a centralized infrastructure will be the main target of rivals in battlefields. If the infrastructure is destroyed, then the whole network may be paralyzed [13]. Furthermore, although prevention-based approaches can prevent misbehaviour, there are still chances remained for malicious nodes to participate in the routing procedure and disturb proper routing establishment. From the experience in the design of security in wired networks, multi-level security mechanisms are needed. In MANETs, this is especially true given the low physical security of mobile devices.[14],[15]. Serving as the second wall of protection, detection-based approaches can effectively help identify malicious activities [16]-[18].

Although some excellent work has been done on detection-based approaches based on trust in MANETs, most of existing approaches do not exploit direct and indirect observation (also called second hand information that is obtained from third party nodes) at the same time to evaluate the trust of an observed node.

In this paper, we interpret trust as the degree of belief that a node performs as expected. Based on this interpretation, we propose a trust management scheme to enhance the security of MANETs. Every node monitors the behaviour of its

neighbours and classifies it as either malicious or non-malicious node. Then the direct observation value is shared among the nodes in the network by piggybacking the observation along the RREQ and RREP packets used for route discovery phase of DSR protocol. Then the source node can get second hand information about the nodes in the selected route using OREQ and OREP packets. Then the source decides the path that is void of any malicious nodes.

We evaluate the proposed scheme in a MANET routing protocol called Dynamic Source Routing with the Network simulator version 2.34. Extensive simulation results show the effectiveness of the proposed scheme. Throughput and packet delivery ratio can be improved significantly, with slightly increased average end-to-end delay and overhead of messages.

The remainder of this paper is organized as follows. Related work is presented in Section II. The trust model and its two components are presented in Section III. Section IV describes the methodology used for computing direct trust. Section V describes the technique used to propagate the trust among other nodes in the network. The indirect observation technique is described in section VII. The performance and effectiveness of our scheme are evaluated and discussed in Section VIII. Finally, we conclude the work in Section IX.

II. RELATED WORK

Trust-based security schemes are important detection-based methods in MANETs, which have been studied recently [19], [20], [22], [24]–[26], [28]–[31]. In [19], [20], the trust value of a node based on direct observation is derived using Bayesian methodology. The authors of [22] regard trust as uncertainty that the observed node performs a task correctly, and entropy is used to formulate a trust model and evaluate trust values by direct observation. In [23] The Cluster Head (CH) monitors its cluster member behaviour. When any misbehaviour is monitored by cluster head means, it sends the request about that misbehaving node to its nearby node (NN) to get the direct trust value (DTV). And also CH sends the request to other cluster members about that misbehaving node. If that cluster members are having value about that misbehaving node means, it sends the indirect trust value to the CH. Otherwise cluster members ignores the request send by CH. This technique is applicable for cluster based MANETs alone and if the cluster head is compromised then the whole cluster will be paralyzed. In [24], the trust value divides the nodes of the network into 3 categories: ally list (level2), associate list(level1), acquaintance list(level0). An additional field "level" is there in neighbour table. When a node has data to send it just checks Its neighbour table, if the destination is available it just sends data packets. If not, it searches for a Node which has route to destination in its same level. If no suitable node is found it goes to Next lower level and so on. But Heavy computation and searching mechanism is needed in this technique which reduces the battery life time of the nodes. The protocol proposed in [25] maintains Confidentiality and authenticates the nodes based on digital Signature and detects the nodes which are misbehaving. This protocol can't detect authenticated malicious node.

Compared to direct observation in trust evaluation, indirect observation or second-hand information can be important to assess the trust of observed nodes. For example, the collection of testimonies from neighbour nodes can detect the situation where a hostile node performs well to one observer, while performing poorly according to another node. Some related works have been done in [26] where the nodes neighbouring to a malicious node initiate trust reports. These trust reports are flooded through the network. a source node can use the trust levels it establishes for other nodes to evaluate the security of routes to destination nodes. But separate control packets are used to disseminate the information which makes the network congested. In our work, the direct observation value is disseminated using the control packets required for route discovery phase so no additional packets are used for sharing the direct trust.

Trust based security systems are also studied in different network architectures, e.g., wireless sensor networks [27], [28], vehicular ad hoc networks (VANETs) [29], cooperative wireless networks [30], etc. Although different types of networks have different specific characteristics, the proposed trust model based on direct and indirect observation is general enough and can be customized to a particular network.

III. TRUST MODEL IN MANETS

In this section, we describe the definition and properties of trust in MANETs. Based on the definition, we depict the trust model that is used to formulate the trust between two nodes in MANETs, and present a framework of the proposed scheme. The main notations that are used in this paper are summarized in Table I.

Table1: Main notations

Notation	Definition
RREQ	Route request
RREP	Route reply
OREQ	Opinion request
OREP	Opinion reply

A. Definition and Properties of Trust:

Trust has different meanings in different disciplines from psychology to economy [28]. The definition of trust in MANETs is similar to the explanation in sociology, where trust is interpreted as degrees of the belief that a node in a network (or an agent in a distributed system) will carry out tasks that it should [28]. Due to the specific characteristics of MANETs, trust in MANETs has five basic properties: subjectivity, dynamicity, non-transitivity, asymmetry, and context-dependency [28]. Subjectivity means that an observer node has a right to determine the trust of an observed node. Different observer nodes may have different trust values of the same observed node. Dynamicity means that the trust of a node should be changed depending on its behaviours. Non-transitivity means that if node A trusts node B and node B trusts node C, then node A does not necessarily trust node C. Asymmetry means that if node A trusts node B, then node B does not necessarily trust node A. Context-dependency means that trust assessment commonly bases on the behaviours of a node. Different aspects of actions can be evaluated by different trust. For example, if a node has less power, then it may not be able to forward messages to its neighbours. In this situation, the trust of power in this node will decline, but the trust of security in this node will not be changed due to its state.

B. Trust Model:

In this model, trust is made up of two components: direct observation trust and indirect observation trust. These components are similar to those used in [42]. In direction observation trust, an observer estimates the trust of his one-hop neighbour based on its own opinion. If we only consider direct observation, there would be prejudice in trust value calculation. In order to obtain less biased trust value, we also consider other observers' opinions. in this paper there are two situations that may severely disturb the effective evidence from neighbours: unreliable neighbours and unreliable observation [29]. Unreliable neighbours themselves are suspects. Even though neighbours are trustworthy, they may also provide unreliable evidence due to observation conditions.

C. Framework of the Proposed Scheme:

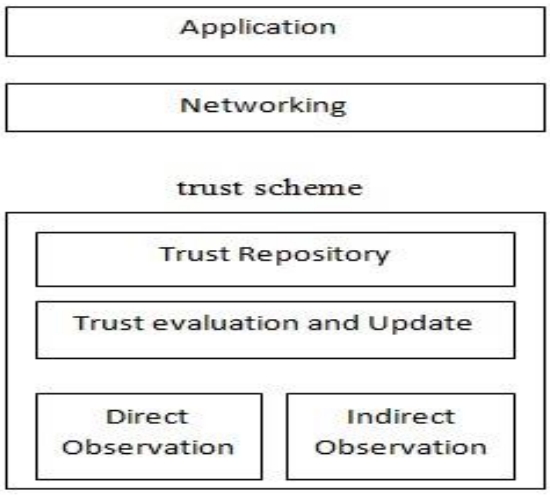

Fig 1: framework of the proposed scheme

In the trust scheme component, the module of trust evaluation and update can obtain evidence from direct and indirect observation modules. Next, the trust values are stored in the module of trust repository. Routing schemes in the networking component can establish secure routing paths between sources and destinations based on the trust repository module. The application component can send data through secure routing paths.

IV. DIRECT OBSERVATION

The malicious nodes in our project are programmed to perform Black hole attack which is a type of denial-of-service attack in which a node acting as a router that is supposed to relay packets instead discards them. Since packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.

In order to detect the malicious behaviour, we have programmed the malicious nodes in such a way they constantly send unwanted Hello messages to its neighbours at constant intervals of time requesting for data transfer. These hello messages are treated as disturbance message by other nodes in the network. The nodes in the network are programmed to maintain a Mali-table (Malicious nodes table) which stores and updates the ID of malicious nodes in the network. The algorithm used in this technique is Mali-detection Algorithm which is described below.

Algorithm 1: MALI-DETECTION ALGORITHM

---

1. Receive packets
2. **if** packet is Hello
   a. Set as disturbance message is received
   b. Start the message count
   c. **if** the message count exceeds threshold(variable)
      i. Check the Mali table
      ii. **if** node not found

Add the node in table
Else
Ignore the message
endif
endif
endif

When a node in the network receives a Hello message packet, the node is assumes the hello message as a disturbance message and it starts the count of the hello message. Sometimes a benign node may falsely forward it but not frequently. So we have set a threshold value for the hello message count. If the number of hello message counts received exceeds a threshold value then the forwarder of hello message is treated to be malicious. Then the observer node checks its Mali-table to find whether there is an entry for that malicious node ID in the Mali-table. If there is no such entry, then the observer node adds the malicious node's ID to its Mali-table. If there is already an entry for that malicious node in the Mali-table, then the hello message is discarded.

V. DIRECT TRUST PROPAGATION

The RREQ and RREP packets used in DSR technique are programmed to include a Mali-list, a list which contains the ID of the malicious nodes. There is no additional packet used for sharing the direct observation information with the neighbours. This prevents the overhead of control packets in the network thereby reducing congestion in the network.

The algorithm used for sharing the direct observation is called as the Mali-share algorithm which is divided into 4 parts

---

Algorithm 2 : MALI-SHARE ALGORITHM PART 1

---

1. **if** node has the data
2. Check route cache
3. **if** route is available

Forward the data
else
Initiate the route discovery
endif

Check the Mali cache
if Mali found
Update the mali info in RREQ
endif
4. Broadcast RREQ
endif

Initially the source checks whether there is a route to the destination by checking its route cache. If there is no route to the destination, it initiates a route discovery process using a RREQ packet as we discussed in previous chapter. If the source node's Mali-table contains any any malicious node's ID, then the source adds the ID of these nodes in the Mali-list of RREQ packet and broadcasts it to the entire network.

Algorithm 3 : MALI-SHARE ALGORITHM PART 2

---**if** RREQ received

1. Check the RREQ
2. **if** Mali_list != Null
   Update Mali-table
   endif
3. check the Mali Table
   if forwarder ∈ table
   Ignore the message
   else
   i. **for** i∈ Mali table
   ii. Updates *"i"* node's id in RREQ
   endif
4. **If** current node == destination of the pkt
   a. RREQ ⇒RREP
   b. update the reverse route info
   c. Send to source
   else
   Broadcast the RREQ as forwarder
   endif

endif

The above algorithm describes the trust propagation in RREQ forwarding phase. Whenever a node receives a RREQ from the source or any other intermediate node,the nodes are programmed to perform two important functions as follows.

A. Mali-list updation

B. Mali-table updation

A. Mali-list Updation:

The node checks whether the Mali_list of the RREQ is Empty. If not then it will obtain the ID of nodes present in the Mali-list of RREQ and update those ID's in its Mali-table. The node also checks whether the ID of forwarder of the RREQ is present in its Mali-table. If yes, it mean that the RREQ is fake since it is from a malicious node. So the node discards the RREQ packet. Otherwise the Mali-list updation process takes place.

B. Mali-table Updation:

If the forwarder of RREQ is found to be benign, then the RREQ received node refers its Mali-table and add the ID of the malicious nodes present in the table to the Mali-list of the RREQ. If the received node (current node) is the destination node, then the RREQ packet is changed to RREP packet, otherwise the node forwards the RREQ packet to other nodes as forwarder.

Algorithm 4 : MALI-SHARE ALGORITHM PART 3

---

if RREP received
1. Check the RREP
2. **if** Mali_list != Null
   Update Mali-table
   endif
3. check the Mali Table
   if forwarder ∈ table
   Ignore the message
   else
   i**. for** i∈ Mali table
   ii. Update *"i"* node's id in RREQ
   endif
4. **if** current node =source of the packet
   a. update the reverse route info
   b. Send to source
   else
   for i ∈ mali-table
   i. Update *"i"* node's id in Mali-list
   ii. Forward RREP
   endif

endif

The above algorithm describes the trust propagation in RREP forwarding phase. After the RREQ packets are broadcasted by the intermediate nodes, the destination node might have received a number of RREQ packets The destination node then checks the path traversed by all the RREQ packets. Then the destination will choose a path which has minimum number of hop count which also may be a shortest path. The destination node then sends reply using RREP packets that contains the reverse route information and the RREP packet traverses along that reverse route only. The RREP packet also contain the Mali-list field which contains the Malicious node ID's that are present in the RREQ packet for which the destination sends the reply. The nodes in the reverse route may have updated their Mali-table by the time the RREQ reaches the destination so it is necessary that the nodes in the route must update the Mali-list of RREP and their own Mali-table while the RREP heads to the source.

When a node receives a RREP packet from the destination or any other intermediate node present in the reverse route, then the node checks the Mal-list of RREP packet is Empty. If not then it will obtain the ID of nodes present in the Mali-list of RREP and update those ID's in its Mali-table. The node also checks whether the ID of forwarder of the RREP is present in its Mali-table. If yes, it mean that the RREP is fake since it is from a malicious node. So the node discards the RREQ packet. If the forwarder of RREQ is found to be benign, then the RREQ received node refers its Mali-table and add the ID of the malicious nodes present in the table to the Mali-list of the RREQ. If the received node (current node) is the destination node, then the RREQ packet is changed to RREP packet, otherwise the node broadcasts the updated RREQ packet to other nodes as a forwarder.

Algorithm 5 : MALI-MAINTENANCE ALGORITHM

---

if Current time > expire time
Delete the Mali ID in Mali-table
endif

The nodes in the network are programmed to refresh the Mali-table after some period of time called as the Expire time. If the ID of a malicious node in the Mali-table is present for a duration greater than the Expire time period, then that malicious node's ID will be deleted from the Mali-table.

VI. INDIRECT OBSERVATION

The Indirect Observation mechanism is achieved using two control packets called Opinion REQuest (OREQ) and Opinion REPly (OREP). These packets also have a Mali-list field which contain the ID of nodes that are present in the selected routes for which recommendation or opinion from other nodes is required by the source. The source upon reception of RREP packet has to check whether the nodes in the route are benign nodes. So the source generates a OREQ packet which contains the ID of nodes that are present in the selected route. This is a second hand confirmation about the activities of the nodes in the selected route. Also the source has to confirm with the destination whether the route in the OREP packet is provided by destination or some change has been done in the reverse route information by the malicious nodes.

So this algorithm is divided into 2 parts.

1. To check the behaviour of nodes in the selected route after receiving RREP packets.
2. To authenticate the selected route with the destination.

Algorithm 6 : MALI-MAINTENANCE ALGORITHM

1.**if** OREQ received
  a. set val = 0
    b**. for** "*i*" ϵ OREQ list
    c. **if** "*i*" ϵMali table
      i. Generate the OREP
      ii. Forward to source of OREQ as OREP
      iii. Set Val = 1
    endif
  2. if val ==0
    broadcast OREQ
  endif
endif

This algorithm is necessary for the source to check whether the nodes in the selected route has been identified as the malicious node after the reception of RREP packets. So the source broadcasts an OREQ packet as discussed above. After broadcasting the OREQ packets, if an intermediate node receives the OREQ packet, then it checks the OREQ-list and if the intermediate node finds any of that node ID present in its Mali-table, then it immediately sends a OREP to source indicating that the selected route contains the malicious node by adding the malicious node's ID in the OREQ mali-list. If there is no such entry, then it forwards the OREQ to other neighbouring nodes.The use of 'val' in the algorithm is to prevent the formation of loops of OREQ packets and the val=1 indicates it as OREP packet and the nodes receiving the OREP packets forward it to the source.

Algorithm 7 : MALI-MAINTENANCE ALGORITHM

---

if OREQ received==destination
  a. Check OREQ list
    i. **if** OREQ list ==reverse route
      1.OREQ => OREP as destination
      2. Forward OREP to source
    else
      1. Add the next min hop route in OREQ-list

2.OREQ => OREP as destination
3. Forward OREP to source
endif
endif

This algorithm is to authenticate the source's selected route with the destination. When the destination receives the OREQ packet the destination checks whether the OREQ-list i.e., the selected route is same as the reverse route as indicated in the RREP packet. If yes the destination will not make any inclusion to OREQ packet and converts the OREQ to OREP and forwards it to the source. The destination also checks the OREQ-list using the Indirect Trust Algorithm- Part 1 and if the list contains any malicious mode as in its Mali-table, then it chooses another minimum hop route and sends it to the source as RREP packet.

VII. SIMULATION RESULTS AND DISCUSSION

The proposed scheme is simulated on the NS-2 platform with the DSR protocol. In the simulations, the effectiveness of the scheme is evaluated in an insecure environment with 1 to 5 malicious nodes. We compare the performance of the proposed scheme with that of direct observation mechanisms with trust propagation.

A. Environment Settings:

We randomly place nodes in the defined area. Each scenario has a pair of nodes as the source and destination with Constant Bit Rate (CBR) traffic. The simulation parameters are listed in Table II. In our simulations, we assume that there are two types of nodes in the network: normal nodes, which follow the routing rules, and compromised nodes, which drop or modify packets maliciously. We also assume that the number of compromised nodes is minor compared to the total number of nodes in the network.

PARAMETER	VALUE
Channel	Wireless channel
Propagation model	Two ray ground
Physical layer type	Wireless
Mac layer	802.11
Transport layer	UDP
Data traffic	CBR
Queue type	Drop tail
Antenna type	Omni-directional
X dimension of the topo	1000
Y dimension of the topo	1000
Number of pckts in queue	50
Number of nodes	50

The nodes are programmed to move at 20 metres/second velocity to random locations. There are four performance metrics considered in the simulations: 1) *Packet delivery ratio (PDR)* is the ratio of the number of data packets received by a destination node and the number of data packets generated by a source node; 2) *Throughput* is the total size of data packets correctly received by a destination node every second; 3) *Average end-to-end delay* is the mean of end-to-end delay between a source node and a destination node with CBR traffic; 4) *Message Overhead* is the size of Type Length Value (TLV) blocks in total messages.

B. Performance Improvement:

The simulation is performed with both direct observation and indirect observation. From the fig 2, it is clear that the Packet Delivery Factor almost equals 100% for most of the time when we use Unified Trust management Scheme(green line) rather than direct observation(red line) alone. The increase in PDF signifies the enhancement of security of the network against the Black hole attack by the malicious nodes. The fig 3 shows that as the number of malicious nodes increases, the delay of packet transmission in case of direct observation (red line) increases whereas the delay is almost

irrespective of the number of malicious nodes in case of unified trust scheme (green line) which includes direct and indirect observations.

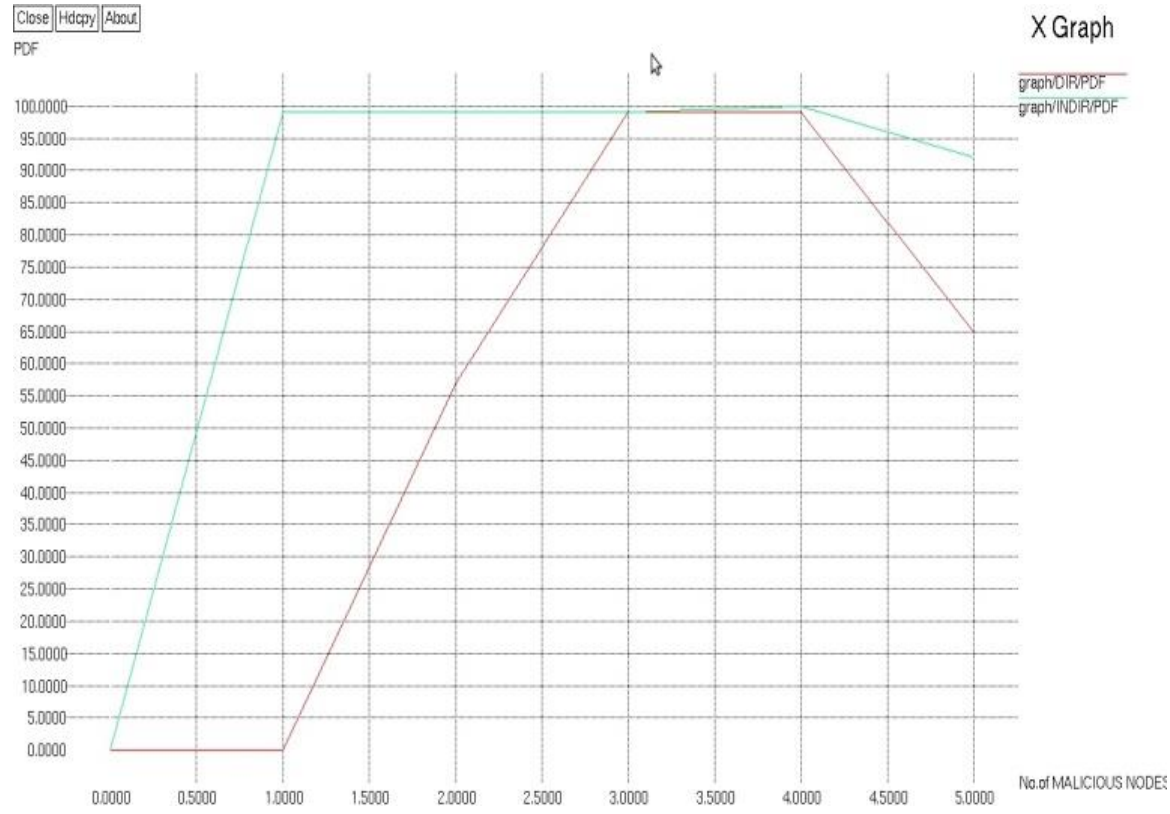

Fig. 2: PDF vs Number of malicious nodes

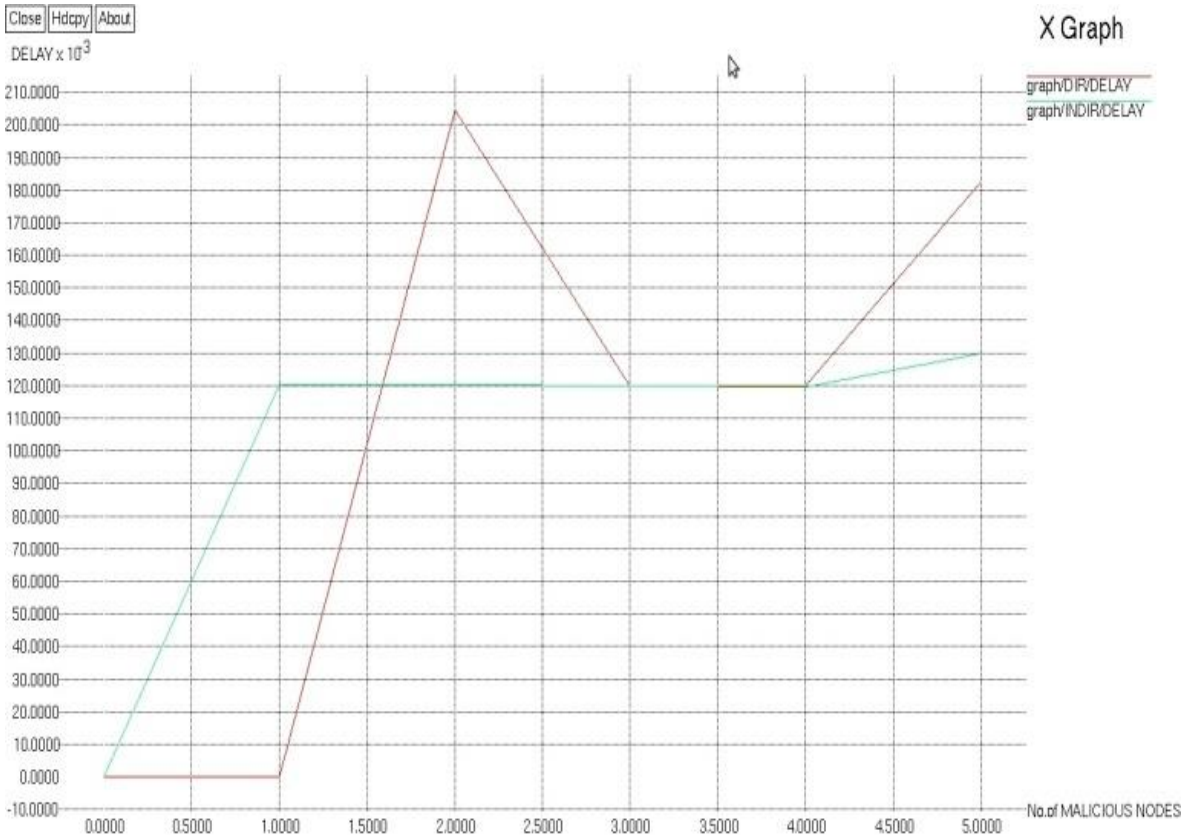

Fig. 3: Delay vs Number of malicious nodes

The fig. 4 given below shows that the jitter value is low without any prevention technique (red bar) and prevention using Indirect observation (blue bar) involves higher jitter value when compared to prevention technique using only direct observation (green bar).

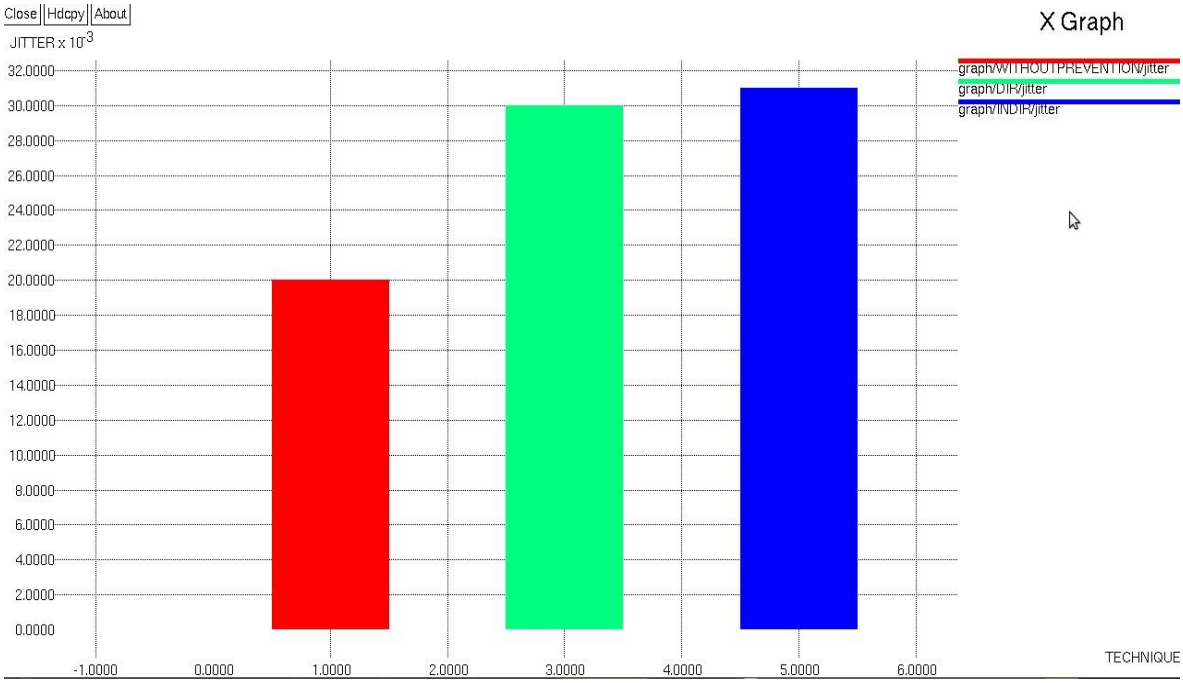

Fig. 4: Jitter vs Technique used

The fig. 5 shows that the number of overhead packets involved for unified trust management scheme(blue line) is higher than direct trust scheme(green line) in most of the cases because of the additional use of OREQ / OREP packets for indirect observation technique..

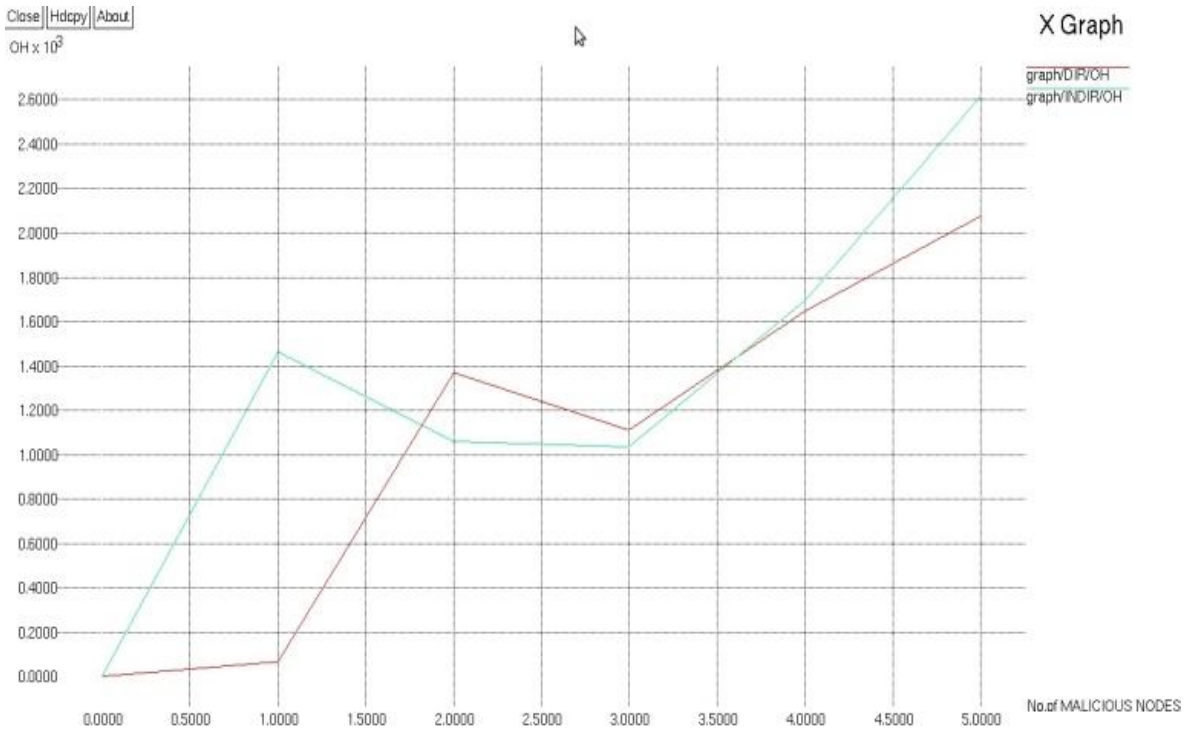

Fig. 5: Control packet overhead vs. Number of malicious nodes

From these four figures, we can observe that our proposed scheme based on indirect trust outperforms the existing scheme significantly in terms of both PDR and throughput. Our scheme takes advantage of trust evaluation of nodes in the

network so that more reliable routing paths can be established. The existing scheme is severely affected by malicious nodes that drop or modify packets. We can observe that the proposed scheme with indirect trust can steer clear of malicious nodes dynamically. Therefore, the PDR and throughput of our scheme are better than those of the existing scheme.

VIII. CONCLUSIONS AND FUTURE WORK

In this paper, we proposed a unified trust management scheme that enhances the security of MANETs. We evaluate the trust values of observed nodes in MANETs. Misbehaviours such as dropping or modifying packets can be detected in our scheme through trust values by direct and indirect observation. Nodes with low trust values will be excluded by the routing algorithm. Therefore, secure routing path can be established in malicious environments. Based on the proposed scheme, more accurate trust can be obtained by considering different types of packets, indirect observation from one-hop neighbours and other important factors such as buffers of queues and states of wireless connections, which may cause dropping packets in friendly nodes. The results of MANET routing scenario positively support the effectiveness and performance of our scheme, which improves throughput and packet delivery ratio considerably, with slightly increased average end-to-end delay and overhead of messages. In our future work, we will extend the proposed scheme to MANETs with cognitive radios.

REFERENCES

[1] S. Corson and J. Macker, "Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations," IETF RFC 2501, Jan. 1999.

[2] F. R. Yu, Cognitive Radio Mobile Ad Hoc Networks. New York: Springer, 2011.

[3] J. Loo, J. Lloret, and J. H. Ortiz, Mobile Ad Hoc Networks: Current Status and Future Trends. CRC Press, 2011.

[4] 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.

[5] 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. Networking, vol. 2013, pp. 188–190, July 2013.

[6] Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," IEEE Trans. Wireless Commun., vol. 13, pp. 1616–1627, March 2014.

[7] J. Chapin and V. W. Chan, "The next 10 years of DoD wireless networking research," in Proc. IEEE Milcom'11, (Baltimore, MD, USA), Nov. 2011.

[8] 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. Tech., vol. 60, pp. 1025 –1036, Mar. 2011.

[9] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: dis-tributed key management for security," in Proc. 2nd OLSR Workshop, (Domaine de Voluceau, France), Dec. 2005.

[10] 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.

[11] Y. Fang, X. Zhu, and Y. Zhang, "Securing resource-constrained wireless ad hoc networks," IEEE Wireless Comm., vol. 16, no. 2, pp. 24–30, 2009.

[12] F. R. Yu, H. Tang, P. Mason, and F. Wang, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks," IEEE Trans. on Network and Service Management, vol. 7, pp. 258 – 267, Dec. 2010.

[13] S. Marti, T. Giuli, K. Lai, and M. Maker, "Mitigating routing misbe-havior in mobile ad hoc networks," in Proc. ACM MobiCom'00, (New York, NY, USA), Aug. 2000.

[14] W. Lou, W. Liu, Y. Zhang, and Y. Fang, "SPREAD: improving network security by multipath routing in mobile ad hoc networks," ACM Wireless Networks, vol. 15, no. 3, pp. 279–294, Mar. 2009.

[15] R. Zhang, Y. Zhang, and Y. Fang, "AOS: An anonymous overlay system for mobile ad hoc networks," ACM

Wireless Networks, vol. 17, no. 4, 843–859, May 2011.

[16] P. Albers, O. Camp, J.-M. Percher, B. Jouga, and L. M. R. S. Puttini, "Security in ad hoc networks: a general intrusion detection architecture enhancing trust based approaches," in Proc. 1st Int'l Workshop on Wireless information Systems, (Ciudad Real, Spain), Apr. 2002.

[17] .A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," IEEE Wireless Comm., vol. 11, pp. 48–60, Feb. 2004.

[18] 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. 10,3064 – 3073, Sept. 2011.

[19] S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in Proc. 2nd Workshop on the Economics of Peer-to-Peer Systems, (Bologna, Italy), Nov. 2004.

[20] C. Zouridaki, B. L. Mark, M. Hejmo, and R. K. Thomas, "A quantita-tive trust establishment framework for reliable data packet delivery in MANETs," in Proc. 3rd ACM Workshop on SASN'05, (Alexandria, VA, USA), Nov. 2005.

[21] Y. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 305–317, 2006.

[22] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the confi-dant protocol," in Proc. ACM MOBIHOC'02, (Lausanne, Switzerland), Jun. 2002

[23] Annadurai, P. And Vijayalaksmi, S In Their Paper '.Identifying Malicious Node Using Trust Value In Cluster Based Manets ' 2013

[24] Edua Elizabeth, N., Radha, S., Priyadarshini, S., Jayasree, S., Naga Swathi, K. Have Proposed 'Srt- Secure Routing Using Trust Levels In Manets' 2012

[25] Sharma, S. Mishra, R. Kaur, .M In Their Paper 'New Trust Based Security Approach For Ad-Hoc Networks' (2010)

[26] Zhaoyu Liu ; Joy, A.W. ; Thompson, R.A. Transactions On Dependable And Secure Computing ' A Dynamic Trust Model For Mobile Ad-Hoc Networks',2004

[27] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the OLSR protocol," in Proc. 2nd IFIP Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net 2003), (Mahdia, Tunisia), Jun. 2003.

[28] T. Clausen and U. Herberg, "Vulnerability analysis of the optimized link state routing protocol version 2 (OLSRv2)," in Proc. IEEE WCNIS'10, (Beijing, China), Feb. 2010.

[29] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc networks," IEEE Comm. Mag., vol. 40, no. 10, pp. 70–75, 2002.

[30] T. Clausen, C. Dearlove, and J. Dean, "Mobile ad hoc network (MANET) neighbourhood discovery protocol (NHDP)," IETF RFC 6130, Apr. 2011.