RESEARCH ARTICLE OPEN ACCESS

Dynamic High Secure Protocol for Mobile Adhoc Network

Aravindan B[1], Dhivakar A[2], Shreehari V.V.[3]

[1,2,3](Computer Science and Engineering, Dhanalakshmi College Of Engineering, Chennai)

Abstract:

The working of MANET protocol, may compromise the security in it. In this paper, we propose a new key exchange method to improve the security of MANETs. In this proposed mechanism we send the key through the control packets instead data packets. By using this mechanism we can ensure that even if the intruder gets access to the data packet he cannot decrypt it because there is no key associated with the packet. Brute force attack also becomes infeasible because the packet is alive in the network for a less time.

Keywords—**Mobile ad hoc networks (MANETs), security, trust management, uncertain reasoning.**

I. INTRODUCTION

With advances in wireless technologies and mobile devices, mobile ad hoc networks (MANETs) [1], [2] have become popular as a communication technology in military environments such as the establishment of communication networks used for cordinating the military deployment among the soldiers, vehicles, and operational command centers [3]. There are many risks in these environments that need to be considered seriously due to the distinctive features of MANETs, including open wireless transmission medium, distributed nature, and lack of centralized infrastructure of security protection [4]–[6]. Therefore, security in MANETs is a challenging research topic [7]. There are two classes of approaches that can safeguard MANETs: prevention-based and detection-based approaches [8]. The Prevention-based approaches are studied comprehensively in MANETs [9]–[12]. One issue of this approach is that the need of a centralized key management infrastructure , which may not be realistic in distributed networks such as MANETs. In addition, this infrastructure will be the main target of rivals in battlefields. If the infrastructure is destroyed, then the whole network may be paralyzed [13]. Although the prevention-based approaches can prevent misbehavior, there are still chances for a malicious nodes to participate in the routing and disturb the proper routing establishment. From the study of design of security in wired networks,we can surely say that multilevel security mechanisms are needed. In MANETs, this is particularly true because of the low physical security of mobile devices [14], [15]. Serving as the second wall of protection, detection-based approaches can effectively help in identifying the malicious activities [16]–[18]. Although there has been research done on detectionbased approaches based on trust in MANETs, most of the existing approaches do not exploit the direct and indirect observations (also called as the secondhand information that is obtained from third-party nodes) at the same time evaluating the trust of an observed node. Moreover, indirect observation in most of the approaches is only used to assess the worthiness of the nodes, which are not in the range of the observer node [19]. Therefore, inaccurate trust values may also be derived. In addition, most methods of trust evaluation from direct observation [19], [20], do not differentiate data packets and control packets. However, in MANETs, control packets usually are more important than data packets. In this paper, we interpret the trust as a degree of belief that a node performs as expected. We also recognize uncertainty in trust evaluation.

Based on this understanding, we propose a trust management scheme to enhance the security of MANETs. The difference between our's and existing schemes is that we use uncertain reasoning to derive trust values. It was initially proposed from the artificial intelligence field to solve the problems in expert systems, which had frequent counterfactual results. The elasticity and flexibility of uncertain reasoning make it successful in many fields, such as expert systems and data fusion. The contributions of this paper are outlined as follows. We propose a key exchange scheme that enhances the security in MANETs.In our proposed scheme, the trust model has two fields: trust from direct observation and trust from indirect observation. In direct observation from an observer node, the trust value is obtained using Bayesian inference, which is a type of a uncertain reasoning when the full probability model can be defined. Whereas, with indirect observation from neighbor nodes of the observer node, the trust value can be derived using the Dempster–Shafer theory (DST), which is another type of uncertain reasoning when the proposition of interest can be obtained by an indirect method.

- The proposed scheme differentiates control packets and data packets and excludes the other causes that result in dropping packets, such as unreliable wireless connections and buffer overflows.
- We evaluate the proposed scheme in a MANET routing protocol, i.e., the Ad hoc On Demand Distance Vector Routing (AODV), with the Qualnet simulator. Extensive simulation results show the effectiveness of our proposed scheme. Throughput and packet delivery ratio (PDR) can be improved significantly, with slight increase in 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. The performance and effectiveness of our scheme are evaluated and discussed in Section V. Finally, we conclude this paper in Section VI.

II. RELATED WORK

Trust-based security schemes are one of the important detection-based methods in MANETs, which have been studied recently [8], [19]. In [19] and [20], the trust value of a node based on direct observation is derived using Bayesian methodology. Sun et al. 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 examination. Compared with direct observation in trust evaluation, indirect observation can be important to assess the trust of observed nodes. For example, the collection of testimonies from neighbor nodes can be used to detect the situation where a hostile node performs well to one observer, while performing poorly in accordance to another node. The DST is regarded as a useful mechanism in uncertain reasoning and is most widely used in expert systems and multiagent systems. In, the DST is used in sensor fusion. Intrusion detection systems (IDSs) [8],apply the DST to assess unreliable information from IDS sensors.

In this paper, we use the uncertain reasoning theory from the field of artificial intelligence to evaluate the trust of nodes in MANETs. Uncertainty is an old setback from the gambler's world. This problem can be handled by probability theory. Reasoning is an-other vital behavior in day to day life. A lot of researchers, even Aristotle (384 BCE–322 BCE) (Greek Philosopher), have tried to understand and formulate it. Reasoning based on uncertainty has been prosperous in the artificial intelligence community due to the development of probability theory and symbolic logic. Probabilistic reasoning is introduced to intelligence systems, which is used to tackle the exceptions in automatic reasoning. To surmount the drawbacks of traditional rule-based systems, which are based on truth tables with no exceptions, probabilistic reasoning is proposed, which describes the uncertainty of knowledge is considered and described as subsets of "possible worlds." Probabilistic reasoning can be used in different areas, from artificial intelligence to philosophy, cognitive psychology, and management science. In the field of security in MANETs, we find that this theory is very suitable for trust evaluation based on the trust interpretation in this paper. Bayesian inference and Dempster–Shafer evidence theory are two approaches in uncertain reasoning. We adopt them to assess the trust of nodes by direct and indirect observations. Trust-based security systems are also considered in different network architectures, e.g., wireless sensor networks, vehicular ad hoc networks, cooperative wireless networks, etc. Although different types of networks have different specific characteristics, the planned trust model based on direct and indirect observations is general enough and can be customized to a particular network. To make it easier to apprehend the proposed trust model, we present an overview of AODV and its vulnerabilities. AODV is a reactive routing protocol. It has four types of control messages for route maintenance, i.e., a HELLO message , RREQ , RREP and RERR . Neighborhood discovery is used to facilitate a node's detection of its onehop neighbors in radio range. HELLO messages, which can carry link status such as symmetric, asymmetric, or multipoint relay, are used in the neighborhood discovery procedure. Through periodically sending HELLO messages , a node can thus establish the bidirectional (symmetric) links with its one-hop neighbors . RREQ - A route request message is transmitted by a node requiring a route to a node.As an optimization AODV uses an expanding ring technique when flooding these messages. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received.Data packets waiting to be transmitted (i.e. the packets that initiated the RREQ) should be buffered locally and transmitted by a FIFO principal when a route is set. RREP - A route reply message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.RERR - Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a ``precursor list", containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination.

Consequently, AODV is vulnerable to various attacks such as wormhole attacks, blackhole attacks, spoofing, jamming, etc. In this paper, our scheme is a security mechanism that mainly protects AODV against two types of misbehavior: dropping of packets and modification of packets. The packet dropping attack is also called a blackhole attack, which is a type of denial-of-service attacks. Modification of packets may have a significant impact on a topology map [9]. By the use of trust evaluation in our scheme, malicious nodes that intentionally drop or modify packets can be detected and kept away.

III. TRUST MODEL IN MOBILE AD HOC NETWORK

Here, we intend to describe the definition and properties of trust in MANETs. Based on the definition, we represent the trust model that is used to devise the trust between two nodes in MANETs and present a framework of the proposed scheme.

A. Definition and Properties of Trust

Trust has different interpretations in different disciplines from psychology to economy. The description of trust in MANETs is similar to the explanation in sociology, where trust is explained as degrees of the belief that a node in a network will carry out tasks that it should. Due to the specific characteristics of MANETs, trust in MANETs has the following five essential properties: subjectivity, dynamicity, nontransitivity, asymmetry, and context dependence. Subjectivity implies that an observer node has a right to determine the trust of an observed node. Different observer nodes may have dissimilar trust values of the same observed node. Dynamicity means that the trust of a node should be altered depending on its behaviors. Nontransitivity means that, if node A trusts node B and node B trusts node C, then node A may not essentially trust node C. Asymmetry means that if node A trusts node B, then node B does not automatically trust node A. Context dependence means that trust assessment is commonly based on the activities of a node. Different aspects of events can be evaluated by different trust. For example, if a node has less amount of power, then it may not be able to forward the messages to its neighbors. In this situation, the trust of power in this node will reduce, but the trust of security in this node will not be changed due to its state. Reputation is another essential model in trust evaluation. Reputation reflects the public opinions from members in a community. In MANETs, reputation can be a compilation of trust from nodes in the network. Reputation is more global than trust from the perspective of the whole network .

B. Trust Model

Based on the meaning and features of trust in MANETs, we evaluate trust in the proposed scheme by a real number T with a continuous value ranging between 0 and 1. Although the trust and trustworthiness may be different in contexts, in which the trustor needs to consider the risk, trust and trustworthiness are treated as same for simplicity in the proposed model. In this, the trust is made up of two components namely, direct observation trust and indirect observation trust. In former, an observer estimates the trust of his one-hop neighbor based on its own judgment. Therefore, the trust value is the anticipation of a subjective probability that a trustor uses to decide whether a trustee is reliable or not. It is similar to firsthand information defined in [19] and [20]. If we only consider direct observation, there would be unfairness in trust value calculation. To obtain less biased trust value, we also consider other observers' opinions in this paper. Al-though opinions of neighbors are introduced in, the method that simply takes arithmetic mean of all trust values is not suffice to reflect the real meaning of other unreliable observers' opinions because there are mainly two situations that may severely disturb the effective evidence from neighbors: unreliable neighbors and unreliable observation. Unreliable neighbors themselves are prime suspects. Even though neighbors are trustworthy, they may also in turn provide unreliable evidence due to observation conditions. The DST is a good candidate to aid in this situation, in which evidence is collected from neighbors that may be unreliable.

C. Framework of the Proposed Scheme

Based upon the trust model, the framework of the proposed scheme is shown in Figure. 1. In the trust scheme component, the module of trust evaluation and update can obtain verification from the direct and indirect observation modules and then utilize these approaches, i.e., Bayesian inference and DST, for calculating and updating the trust values. Next, the trust values are stored in the module of trust repository. Routing schemes in the networking module can establish secure routing paths between sources and destinations based on the trust repository module. Then the application component can send data through secure routing paths.

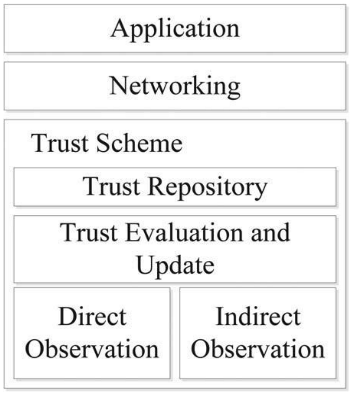


Fig. 1 Framework of the proposed scheme.

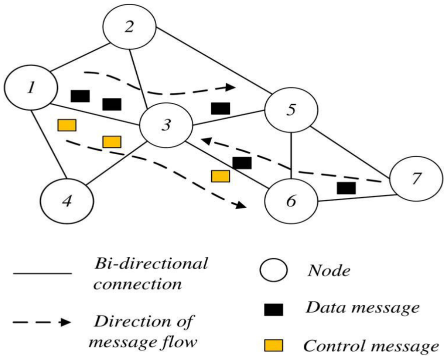


Fig. 2 Example mobile ad hoc network

To explain the basic operation of trust evaluation in our scenario, an example network is shown in Figure. 2. In this example we have taken, node 1 is an observer node, and node 3 as an observed node.

Node 1 sends data messages to node 5 through the node 3. When node 3 receives data messages and forwards it to node 5, node 1 can overhear it. Then, node 1 can calculate the trust value

of node 3 based on the data messages. The same idea is applied to the control message situation. Meanwhile, node 1 can gather information from nodes 2 and 4, which have interactions with node 3 to evaluate the trust value of node 3. This information gathered from third-party nodes is called as the indirection observation. In another situation, node 7 sends the data messages to node 3, which is the destination node. Node 1 cannot overhear the data messages sent to node 3 in this situation.

IV. SECURE ROUTING BASED ON TRUST

The original AODV protocol does not provide security measurements in the protocol. AODV assumes that every node in the network is cooperative and helping. However, this assumption is inappropriate in a military environment. Malicious nodes can even attack the nodes that are not protected. Based on trust values, a secure route can be established. Modifications of AODV consists of two important parts: route selection process based on link metrics and trust-value calculation algorithms. Although the AODV provides new attributes such as link metrics and extensible message formats, which may be efficiently used to improve the security of the protocol, AODV implementation still attempts to use the hop count method when the shortest routing path is calculated. To implement the route selection process based on link metrics, there are three components that need to be changed, i.e., HELLO messages, protocol information bases, and the shortest path algorithm. The message format is also extensible and flexible in AODV. Thus, the information on link metrics can also be added to messages as the type length value (TLV) blocks. Modification of protocol information bases, including the local information base, neighbor information base, and topology information base, is used to record link metrics for each node. Based on these valuable information bases, a route processing set can update the shortest routing path with link metrics. In the ad hoc on demand vector routing protocol (AODV) [43], the trust management scheme can also differentiate the control messages, e.g., route requests and route replies in AODV, by message type checking when a trust evaluation procedure is performed. We assume that each node works in the promiscuous mode implemented by the medium-accesscontrol layer. We also assume that, in a particular time slot, the observed node (sender) does not move out of the transmission range. As the time of packets processing in a node is very short, our assumptions are very realistic in practical networks. This implies that the observer can detect whether the neighboring node sends the received packets before the observed node moves out the transmission range.

Each node needs to record its one-hop neighbors, how many data packets each neighbor received, the number of control packets each neighbor received, how many data packets each neighbor forwards correctly, and the number of control packets each neighbor forwards correctly. When a particular node receives a packet, the number of received packets, according to the kind, will increase one. If the node forwards the received packet correctly, then the number of forwarded packets will in turn increase by one. There are three scenarios under which the number of received packets will not increase. First, if the packet is dropped because of time to live (TTL), then the number of received packets cannot increase. The second scenario is that , if a node that receives a packet drops it due to the overflow of buffers. Third, a packet is dropped by a node because the condition of wireless connection is appalling. Considering these stated significant factors, we improve the accuracy of trust calculation. In this paper, we consider the condition that packets are dropped due to the unreliable wireless connections. During the trust evaluation with direct observation, the model can remove the number of packets dropped by this condition (see Algorithm 1). We suppose that there is a probability that packets are dropped because of unreliable wireless connections. Algorithm 1 describes the details of each iteration. Algorithm 2 describes that an observer node collects evidence from its one-hop neighbors linking the observer node and the observed node. Then, the trust values from indirect observation are evaluated by (18).

After T S and T N are obtained, we can get the total trust value of the observed node by (1). In reactive routing protocols, such as AODV, an observer node can obtain the information from its neighbor nodes periodically by the use of control messages (e.g., HELLO), which can be used to carry the trust values

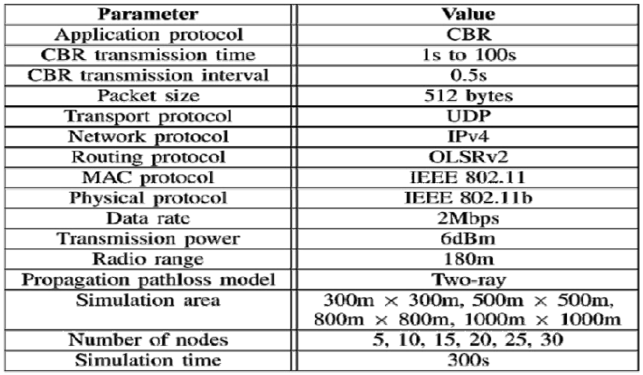
Algorithm 1 Trust Calculation with Direct Observation

```
if node A, which is an observer, finds that its one-hop
   neighbor, Node B that is a trustee, receives a packet then
    the number of packets received increases one
    if node A finds that node B forwards the packet suc-
    cessfully then
      the number of packets forwarded increases one
    else
      if TTL of the packet becomes zero or overflow of
      buffers in node B or the state of wireless connection
      of node B is bad then
        the number of packets received decreases one
      end if
    end if
end if
calculate the trust value $T^S$ from (8) and update the old
   one.
```

Algorithm 2 Trust Calculation with Indirect Observation

```
if node A, which is an observer, has more than one one-
hop neighbors between it and the trustee, node B then
  calculates the trust value $T^N$ from (18)
else
  set $T^N$ to 0
  set $\lambda$ to 1
end if
```

TABLE I
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	OLSRv2
MAC protocol	IEEE 802.11
Physical protocol	IEEE 802.11b
Data rate	2Mbps
Transmission power	6dBm
Radio range	180m
Propagation pathloss model	Two-ray
Simulation area	300m × 300m, 500m × 500m, 800m × 800m, 1000m × 1000m
Number of nodes	5, 10, 15, 20, 25, 30
Simulation time	300s

minimization is used in the Dijkstra' algorithm (e.g., to find the shortest path with the minimal hop count in traditional AODV), we 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, we define the untrustworthy value between nodes A and B as UAB , which can be calculated as UAB = 1 − TAB . The sum of untrustworthy values of a path is

$U_{path}=\sum U\ n-1\ i-1\ kiki + 1=\sum(1-Tkiki + 1)\ n-1\ i-1$ (19) where Tkiki+1 is the trust value between node ki and its one-hop neighbor node ki+1. Nodes k1, k2, . . . , kn

belong to the path with n − 1 hops. The best routing path satisfies the minimum of U path. The trust values and routing table of each node can be stored in the Trusted Platform Module (TPM), which provides additional security protection in open environments with the combination of software and hardware. Since the trust values in each node are the key facilities to detect malicious nodes, the TPM is able to provide effective protection to secure routing and avoid malicious attacks by enemies in battlefields.

V. SIMULATION RESULTS AND DISCUSSIONS

The proposed mechanism is implemented as simulation on the Qualnet platform with the AODV protocol. In the simulations, the effectiveness of the mechanism is evaluated in an not safety environment. We compare the performance of the proposed scheme with that of AODV without security methods.

A. Environment Settings

We randomly place nodes in the defined area. Each scene has two nodes as the source and destination with constant bit rate (CBR) traffic. The simulation parameters are listed in Table II. In our implementation through simulations , we assume that there are two types of nodes in the network: normal nodes, which follow the path of routing rules, and compromised nodes, which drop or modify packets maliciously. We also assume that the number of compromised nodes is less compared with the total number of nodes in the network. In this adversary mode, the proposed scheme is corrected and compared with the original AODV protocol. We have simulated networks with different numbers of nodes. Figure. 3 is an example of the network setup where node 1 is the source node that generates the CBR traffic, node 3 is the destination node, and node 2 is compromised by an adversary. For node mobility, the random waypoint mobility model is adopted and used in a 30-node MANET. The maximum velocity of each node is set from 0 to 10 m/s. The pause time is 30 s. There are five types of performance metrics considered in the simulations: 1) PDR, which 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, which is the overall size of data packets correctly received by a destination node ev-ery second; 3) average end-to-end delay, which is the mean of end-to-end delay between a source node and a destination node with CBR traffic; 4) message overflow, which is the size of TLV blocks in total messages that are used to carry trust values; and 5) routing load, which is the ratio of the number of control packets transmitted by nodes to the number of data packets received successfully to the respective destinations during the simulation.

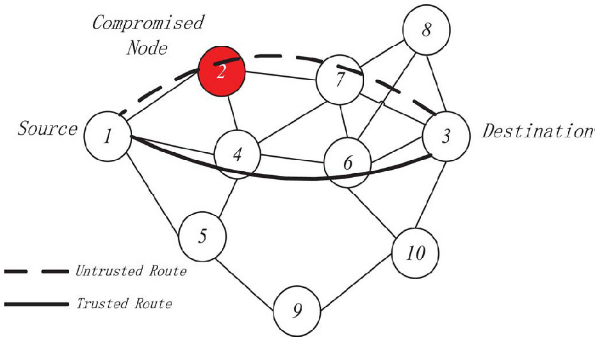


Fig. 3 Example of the network setup

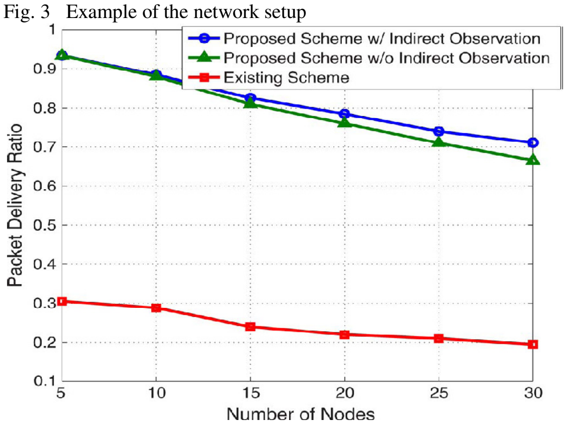


Fig. 4 PDR versus the number of nodes in the network

B. Performance Improvement

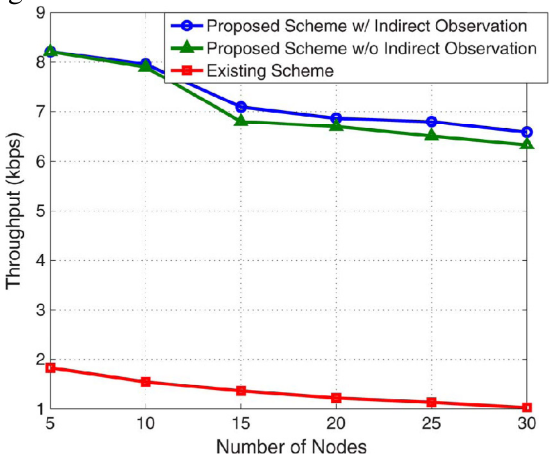


Fig. 5 Throughput versus the number of nodes in the network

The original AODV and our proposed mechanism are evaluated in the simulations, where some nodes misbehave through dropping or modifying packets. In Figure. 4, we compare our scheme with and without indirect observation and original AODV in scenarios under which a source node sends data packets to a destination node in the network, which includes nodes from 5 to 30. In Figure. 4, it is shown that the proposed scheme has a much higher PDR than the existing scheme because the trust-based routing calculation can detect the malfunctioning of malicious nodes. The results also demonstrate that the proposed scheme with indirect observation has the greater PDR among these three schemes. In Figure. 4, we can also find that the PDR of three mechanisms decreases gradually when the number of nodes grows. This is because the collision of sending messages becomes more often as the number of nodes increases in the MANET. Although the PDR declines in three schemes, the proposed mechanism is apparently better than the existing scheme. In Figure. 5, we evaluate throughput in our scheme and the exact and original one. Although the number of packets received correctly decreases as long as the number of nodes increases, the performance of our mechanism has a big improvement. Figures. 4 and 5 both reveal that the trust-based routing algorithm can improve the performance of AODV. Figures. 6 and 7 show the impact of node mobility in a 30node MANET. We can able to see that, as the node velocity increases, PDR and throughput decrease gradually. This is because the greater speed of a node may improve the probability of packets lost. Nevertheless, the proposed scheme performs better than the existing one.

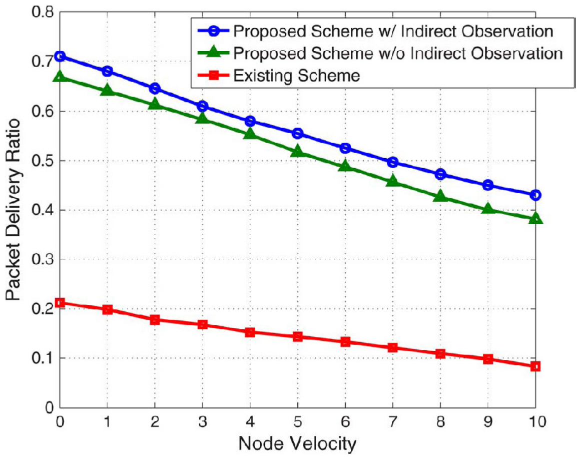


Fig. 6 PDRatio versus node velocity

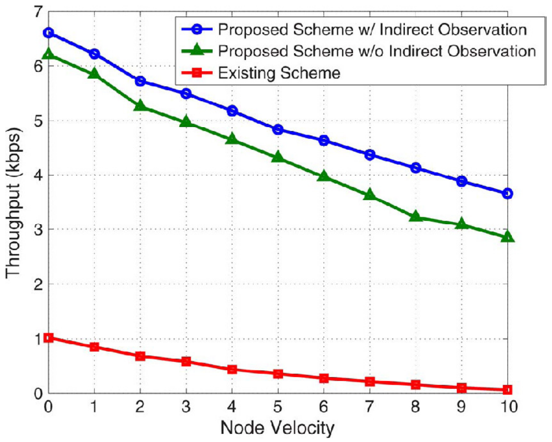


Fig. 7 Throughput versus node velocity

The number of malicious nodes in the MANET also has a significant impact on the throughput of the network. Here, we assume the attackers are independent. Hence, there is no collusion attack in the MANET. We investigate the throughput with malicious nodes, from 2 to 10, in a 30node MANET environment. The basic parameter is the same as that given earlier. Figure. 8 shows that, as the number of malicious nodes increases, the throughput drops dramatically. When the number of malicious nodes reaches to one third of the total number of nodes in the network, the throughput decreases to about half of the throughput in the network with two malicious nodes. From this figures, we can see that the proposed scheme is affected deeply by the number of malicious nodes. Compared with the proposed scheme, the existing scheme has a very low throughput, even if the number of malicious nodes is very small.

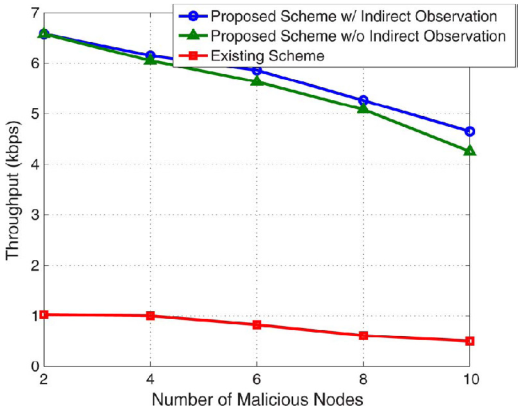


Fig. 8 Throughput versus the number of malicious nodes in the network.

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

Fig. 9 Average end-to-end delay versus the number of nodes in the network

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 trust can steer clear of malicious nodes dynamically. Therefore, the PDR and throughput of our scheme are better than those of the existing scheme.

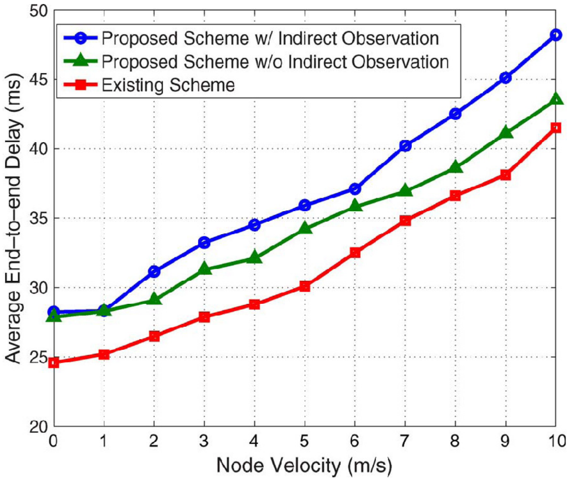
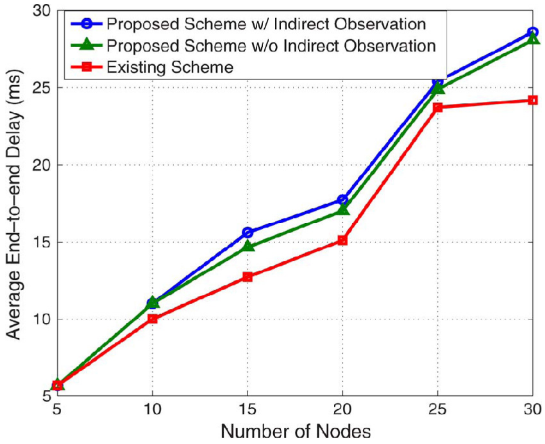


Fig. 10 Average end-to-end delay versus node velocities.

C. Cost

The cost of security enhancement in AODV mainly includes the increased average end-to-end delay and overhead of messages that are used to carry trust values of nodes. Figure. 9 shows that the proposed scheme has a slightly higher average end-to-end delay than the existing mechanism in the malicious environment. In Figure. 10, we can see that, as the node velocity improves, the average end-to-end delay becomes longer. The reason is that trust-based routing path is usually a longer route from a source node to a destination node. Therefore, there is a trivial delay introduced by the proposed scheme. Nevertheless, greater security is guaranteed in the proposed scheme.



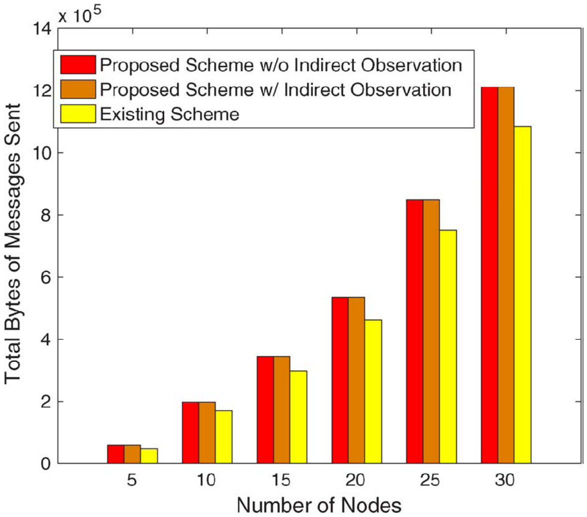


Fig. 11 Total bytes of messages sent versus the number of nodes in the network

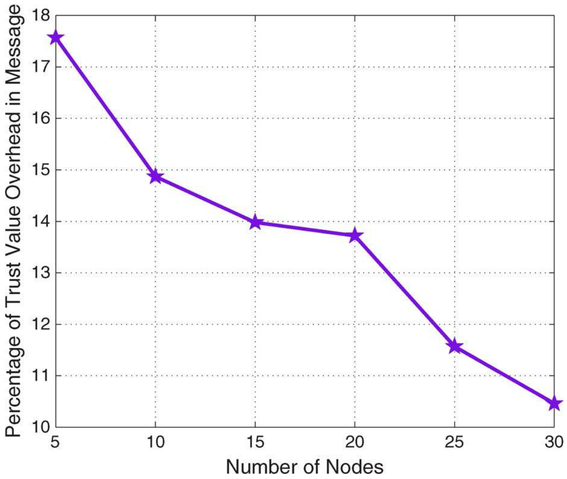


Fig. 12 Percentage of overhead in message versus the number of nodes in the network.

Compared with local computing capacity, sending and receiving message is an important issue in MANETs because message transmission is energy consuming. Thus, we study how much overhead of messages is imported when the trust value is calculated in the AODV protocol. Since the metric link value is introduced in AODV, one new address block TLV, which occupies 12 B, is added to the message format described in Section VI. Figure. 11 shows how much the overhead of messages is imported compared with the original version of AODV. Because trust values are embedded in the HELLO messages, there is no more messages that need to be sent. The overhead is not very high. However, as the number of nodes increases, the percentage of overhead in messages drops dramatically, as shown in Figure. 12. This is because, when the number of nodes increases, the total message becomes large. Then, the 12-B overhead is trivial compared with the size of messages. The results also demonstrate that the proposed mechanism has a lower routing load because of the higher number of packets received correctly by the destination node. As the number of nodes increases, the routing path load of the existing and proposed schemes climb up due to the nature of the reactive routing protocol: time interval generation of control messages in every node.

VI. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a new key exchange mechanism in which the key is sent through the control packets instead of the data packets, by this the intruder cannot decrypt the data because the key sent with the

control packets is alive for a very less time in the network and the data packet which contains the encrypted data cannot be decrypted because due to in availability of key associated with the packet. Brute force attack also becomes infeasible because is alive for a very less time in the network. This key exchange scheme can implemented with any protocol to enhance the security of it and can be used for normal use and exclusively for the defence communication and any other situation which requires high security.

REFERENCES

1. *S.CorsonandJ.Macker,MobileAdHocNetworking(MANET):Routing protocol performance issues and evaluation considerations, Jan. 1999, IETF RFC 2501.*
2. *F. R. Yu, Cognitive Radio Mobile Ad Hoc Networks. New York, NY, USA: Springer-Verlag, 2011.*
3. *J.Loo,J.Lloret,andJ.H.Ortiz,MobileAdHocNetworks: CurrentStatus and Future Trends. Boca Raton, FL, USA: CRC, 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, no. 6, pp. 2674–2685, Jul. 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. Netw., vol. 2013, pp. 188–190, Jul. 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, no. 3, pp. 1616–1627, Mar. 2014.*
7. *J.ChapinandV.W.Chan,"Thenext10yearsofDoDwireless networking research," in Proc. IEEE Milcom, Nov. 2011, pp. 2155–2245.*
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. Technol., vol. 60, no. 3, pp. 1025–1036, Mar. 2011.*
9. *C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: Distributed key management for security," presented at the 2nd OLSR Interop/Workshop, Palaiseau, 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 Secure Comput., vol. 3, no. 4, pp. 386–399, Oct.–Dec. 2006.*
11. *Y. Fang, X. Zhu, and Y. Zhang, "Securing resourceconstrained wireless ad hoc networks," IEEE Wireless Comm., vol. 16, no. 2, pp. 24–30, Apr. 2009.*
12. *F. R. Yu, H. Tang, P. Mason, and F. Wang, "A hierarchical identity based keymanagementschemeintacticalmobileadhocnetworks,"IEEETrans. Netw. Serv. Manag., vol. 7, no. 4, pp. 258– 267, Dec. 2010.*
13. *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.*
14. *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.*
15. *R. Zhang, Y. Zhang, and Y. Fang, "AOS: An anonymous overlay system formobileadhocnetworks,"ACMWirelessNetw.,vol.17,no. 4,pp.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," presented at the 1st Int. Workshop Wireless Inf. Syst., 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, no. 1, 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, no. 9, pp. 3064–3073, Sep. 2011.*

19. *S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in Proc. 2nd Workshop Econom. Peer-toPeer Syst., Nov. 2004, pp. 1–6.*

20. *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.*