ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

Unified Trust Management Scheme that Enhances Security in MANET Using Uncertain Reasoning

Thamayanthi.M[1], Arumai Ruban.J[2]

Student, Computer Science and Engineering, St.Joseph's College of Engineering and Technology, Thanjavur,India[1]

Asst.Prof., Computer Science and Engineering, St.Joseph's College of Engineering and Technology,Thanjavur,India[2]

Abstract: Uncertain reasoning which is from artificial intelligence community, a unified trust management scheme that enhances the security in MANETs is proposed. In the proposed trust management scheme, the trust model has two components: trust from direct observation and trust from indirect observation. In direct observation from an observer node, the trust value is derived using Bayesian inference, when the full probability model can be defined. On the other hand, with indirect observation that is obtained from neighbour nodes of the observer node, the trust value is derived using the Dempster-Shafer theory (DST), which is another type of uncertain reasoning when the proposition of interest can be derived by an indirect method. Combining these two components in the trust model, we can obtain more accurate trust values of the observed nodes in MANETs. Evaluating our scheme under the scenario of MANET routing is also done. The number of nodes used as an intermediary can also be reduced by using beacon messages between them.

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

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. 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. Therefore, security in tactical MANETs is a challenging research topic . There are two complementary classes of approaches that can safeguard tactical MANETs: *prevention-based* and *detection based* approaches. Prevention-based approaches are studied comprehensively in MANETs. One issue of these prevention-based approaches is that a centralized key management infrastructure is needed, 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 . Furthermore, although prevention-based approaches can prevent misbehavior, 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.

Serving as the second wall of protection, detection-based approaches can effectively help identify malicious activities. 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. Moreover, indirect observation in most approaches is only used to assess the reliability of nodes, which are not in the range of the observer node . Therefore, inaccurate trust values may be derived. In addition, most methods of trust evaluation from direct observation 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 trust as the degree of belief that a node performs as expected. We also recognize uncertainty in trust evaluation. Based on this interpretation, we propose a trust management scheme to enhance the security of MANETs. The difference between our scheme and existing schemes is that we use uncertain reasoning to derive trust values. Uncertain reasoning was initially proposed from the artificial intelligence community to solve the problems in expert systems, which have frequent counter-factual results. The elasticity and flexibility of uncertain reasoning make it successful in many fields, such as expert systems, multiagent systems, and data fusion. The contributions of this paper are outlined as follows:

- We propose a unified trust management scheme that enhances the security in MANETs using uncertain reasoning. In the proposed scheme, the trust model has two components: trust from direct observation and trust from indirect observation. With direct observation from an observer node, the trust value is derived using Bayesian inference, which is a type of uncertain reasoning when the full probability model can be defined. On the other hand, with indirect observation from neighbor nodes of the

DOI 10.17148/IJARCCE.2015.4246

observer node, the trust value is derived using the Dempster-Shafer theory, which is another type of uncertain reasoning when the proposition of interest can be derived by an indirect method.

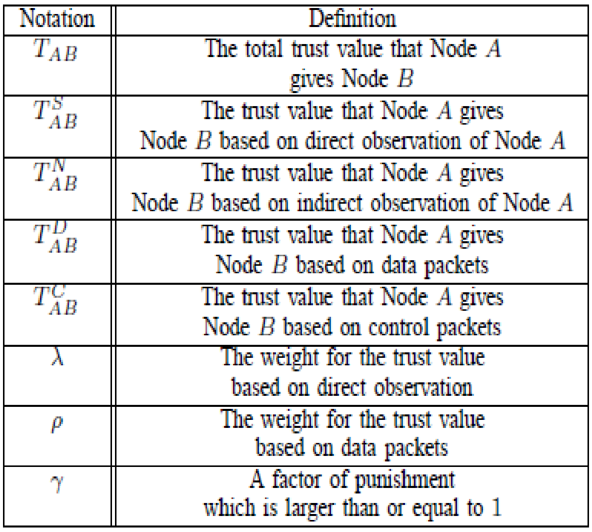
- The proposed scheme differentiates data packets and control packets, and meanwhile excludes the other causes that result in dropping packets, such as unreliable wireless connections and buffer overflows.
- We evaluate the proposed scheme in a MANET routing protocol, the optimized link state routing protocol version 2 (OLSRv2) [27], with the Qualnet simulator. 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.

RELATED WORK

Trust-based security schemes are important detection-based methods in MANETs, which have been studied recently [19], [20], [22], [24]–[26]. 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. 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 neighbor nodes can detect the situation where a hostile node performs well to one observer, while performing poorly according to another node.

In this paper, we use uncertain reasoning theory from artificial intelligence to evaluate the trust of nodes in MANETs. Uncertainty is an old problem from gambler's world. This problem can be handled by probability theory. Reasoning is another important behavior in everyday life.

TABLE I
MAIN NOTATIONS



Notation	Definition
T_{AB}	The total trust value that Node A gives Node B
T^{S}_{AB}	The trust value that Node A gives Node B based on direct observation of Node A
T^{N}_{AB}	The trust value that Node A gives Node B based on indirect observation of Node A
T^{D}_{AB}	The trust value that Node A gives Node B based on data packets
T^{C}_{AB}	The trust value that Node A gives Node B based on control packets
λ	The weight for the trust value based on direct observation
ρ	The weight for the trust value based on data packets
γ	A factor of punishment which is larger than or equal to 1

A lot of researchers, even Aristotle (384 BCE - 322 BCE) (Greek Philosopher), try 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 can be used to different areas, from artificial intelligence to philosophy, cognitive psychology, and management science.

In the area 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 by direct and indirect observations. Direct Observation is made by the observer node, whereas the Indirect Observation is made by the neighbour nodes of the observer node and the trust values are calculated by the respective nodes based on the weight of packet it sends.

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.

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 behaviors.

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 behaviors 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 neighbors. 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. Reputation is another important concept in trust evaluation. Reputation reflects the public opinions from members in a community [41]. In MANETs, reputation can be a collection of trust from nodes in the network. Reputation is more global than trust from the perspective of the whole network

Trust Model

Based on the definition and properties of trust in MANETs, we evaluate trust in the proposed scheme by a real number, T, with a continuous value between 0 and 1. Although trust and trustworthiness may be different in contexts, in which the trust or needs to consider risk [28], trust and trustworthiness are treated the same for simplicity in the proposed scheme. 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. Therefore, the trust value is the expectation of a subjective probability that a trustor uses to decide whether or not a trustee is reliable. It is similar to firsthand information defined by [19], [20].

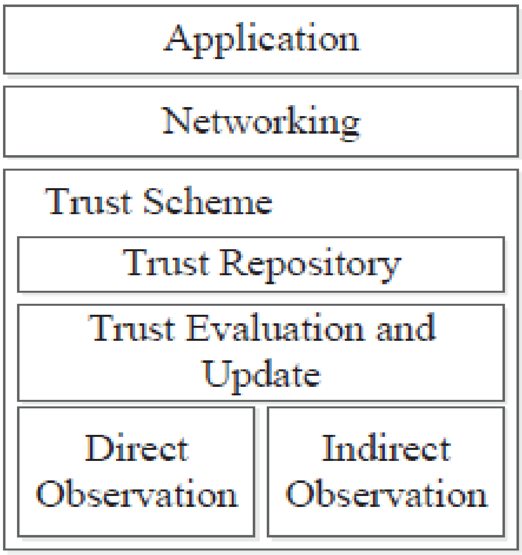


Fig. 1. The framework of the proposed scheme

We denote T_S as a trust value from direct observation and can be calculated by Bayesian inference. The detailed explanation is in Section IV. 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.

Unreliable neighbors themselves are suspects. Even though neighbors are trustworthy, they may also provide unreliable evidence due to observation conditions. The Dempster-Shafer theory [25], [29] is a good candidate to aid in this situation, in which evidence is collected from neighbors that may be unreliable. Therefore, We denote the trust value derived from indirect observation of one-hop neighbors as T_N. Combining the trust value, T_S, from direct observation and the trust value, T_N, from indirect observation, we can get a more realistic and accurate trust value of a node in MANETs..

$$T = \lambda T^s + (1 - \lambda)T^N$$

where λ is a weight assigned to T^S $0 \le \lambda \le 1$.

Framework of the Proposed Scheme

Based on the trust model, the framework of the proposed scheme is shown in Fig. 1. In the trust scheme component, the module of trust evaluation and update can obtain evidence from direct and indirect observation modules and then utilize two approaches, Bayesian inference and DST, to calculate and update the trust values. 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. The trust from direct observation between an observer node A and an observed node B in this trust scheme can be defined further as

$$T^S{}_{AB} = \rho T^D{}_{AB} + (1 - \rho) T^C{}_{AB}$$

where ρ $(0 \le \rho \le 1)$is the weight for data packets; $T^D{}_{AB}$ is the trust value based on data packets; $T^C{}_{AB}$ is the trust value based on control packets. Trust from indirect observation between an observer node A and an observed node B, denoted as $T^N{}_{AB}$, can be obtained by DST. In order to explain the basic procedure of trust evaluation in our scenario, an example network is shown in Fig. 2.

In this example, node 1 is an observer node and node 3 is an observed node. Node 1 sends data messages to node 5 through node 3. When node 3 receives data messages and forwards to node 5, node 1 can overhear it. Then node 1 can calculate the trust value of node 3 based on data messages. The same idea is applied to the control message situation.

In the meanwhile, node 1 can collect information from node 2 and node 4, which have interactions with node 3 in order to evaluate the trust value of node 3. This information collected from third party nodes is called indirection observation. In another situation, node 7 sends data messages to node 3, which is the destination node. Node 1 cannot overhear the data messages sent to node 3 in this situation.

TRUST EVALUATION WITH DIRECT OBSERVATION

Based on the model presented in the last section, we evaluate trust values with direct observation on two malicious behaviors: dropping packets and modifying packets.

In the direct observation, we assume that each observer can overhear packets forwarded by an observed node and compare them with original packets so that the observer can identify the malicious behaviors of the observed node.

Therefore, the observer node can calculate trust values of its neighbors by using Bayesian inference, which is a general framework to deduce the estimation of the unknown probability by using observation.

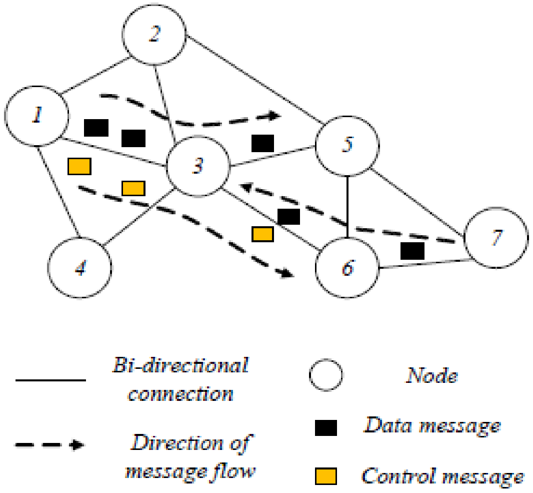


Fig. 2. An example mobile ad hoc network.

As mentioned in the last section of trust model, the degree of belief is a random variable, denoted by Θ and 0 ≤ *θ* ≤ 1. From Bayes' theorem, we can derive the following formulation.

$$f\,(\theta,y|x)= \frac{p(x\ \ \theta,y)\ f(\theta,\ y)}{\int_0^1 p(x|\,\theta,\ y)\ f(\theta,\ y)\ d\theta}$$

where *x* is the number of packets is forwarded correctly; *y* is the number of packets is received by a node; *p*(*x*|*θ, y*) is the likelihood function, which follows a binomial distribution. The factor of punishment makes the trust evaluation more realistic. The punishment factor, *γ*, in the formula of trust evaluation in is described as follows.

$$En[\Theta]= \frac{\alpha_n}{\alpha_n + \gamma\ \beta_n}$$

where *γ* ≥ 1. As the value of *γ* becomes larger, the trust value declines more. This is because the punishment factor gives more weight to misbehavior.

TRUST EVALUATION WITH INDIRECT OBSERVATION

In this section, indirect observation from neighbor nodes used to evaluate the trust value of the observed node will be discussed. Although direct observation from an observer is important in assessing the trust value of the observed node, the testimonies from neighbor nodes are also helpful to judge the trustworthiness of the observed node. Collection of neighbors' opinions can help in justifying whether or not a node is hostile. This mechanism may reduce the bias from an observer. A situation in which a node is benign to one node but malicious to others may be mitigated. In order to implement this method, the Dempster-Shafer theory, which is a mathematical theory of evidence, is used as it is well developed for coping with uncertainty or ignorance, and it provides a numerical measurement of degrees of belief about a proposition from multiple sources [26], [30]. The core of this theory is the belief function that is based on two essential ideas: degrees of belief about a proposition can be obtained from subjective probabilities of a related question, and these degrees of belief can be combined together on condition that they are from independence evidence. In the indirect observation, we assume that there are more than one neighbour nodes between an observer and an observed node when the trust evaluation is performed with DST.

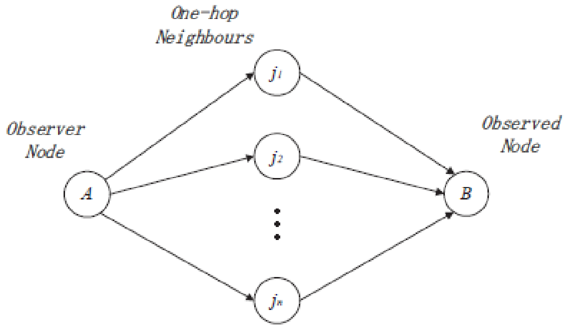


Fig. 3. A scenario for indirect observation

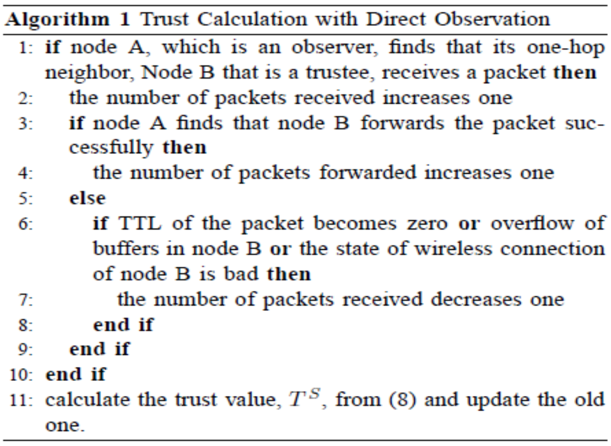
We also assume that evidence provided by different neighbors is independent. First, we will introduce the theory of belief functions. Then we will discuss the rule of combining belief functions that are used to accommodate testimonies from one-hop neighbour nodes in order to assess trust values of nodes in MANETs.

SECURE ROUTING BASED ON TRUST

The original OLSRv2 [27] does not provide security measurements in the protocol. OLSRv2 assumes that every node is cooperative and benevolent. However, this assumption is inappropriate in a military environment. Malicious nodes can attack nodes that are not protected. Based on trust values, a secure route can be established. Modifications of OLSRv2 include two important parts: route selection process based on link metrics and trust value calculation algorithms. Although OLSRv2 provides new features such as link metrics and extensible message formats, which may be used to improve security of the protocol, OLSRv2 implementation [27] [43] still attempts to use hop count when the shortest routing path is calculated. In order to implement route selection process based on link metrics, there are three components that need to be changed, HELLO and TC messages, protocol information bases, and the shortest path algorithm.

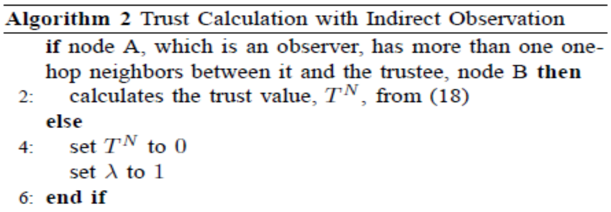
Message format is extensible and flexible in OLSRv2. Thus link metrics information can be added to messages as Type Length Value (TLV) blocks. Modification of protocol information bases, including local information base, neighbor information base and topology information base, is used to record link metrics in each node. Based on these information bases, route processing set can update the shortest routing path with link metrics. Based on the Internet draft of OLSRv2 [27], there are two types of control messages, HELLO and TC. In this trust management, we only consider the TC messages because of the need for forwarding TC. The message type of TC, which is defined in OLSRv2 Internet draft, can be used to check the type of the message. The trust management scheme can separate the data and control messages by the message type during trust evaluation.

DOI 10.17148/IJARCCE.2015.4246



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
```

For other standard protocols, like AODV [44], the trust management scheme also can differentiate the control messages, e.g., RREQs, RREPs in AODV, by message type checking when a trust evaluation procedure is performed.

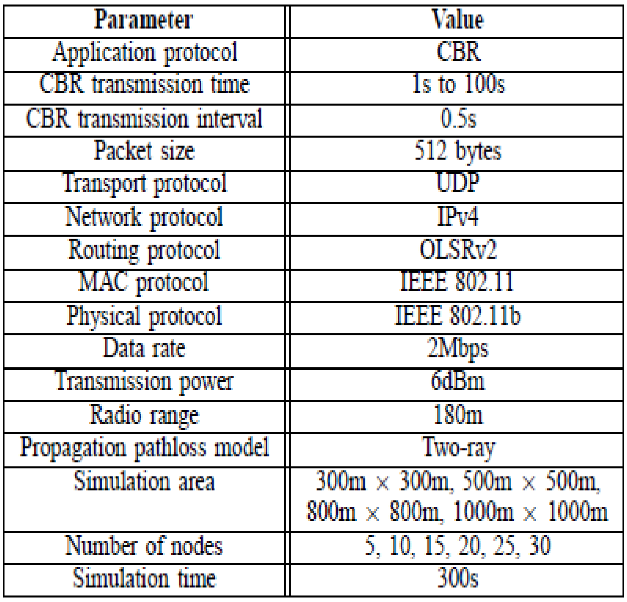
Every node needs to record its one-hop neighbors, how many data packets each neighbor received, how many control packets each neighbor received, how many data packets each neighbor forwards correctly, and how many control packets each neighbor forwards correctly. In OLSRv2, there are two types of control messages: HELLO and TC. TC message is only recorded for trust evaluation because HELLO message is transmitted with one hop in the network. When a node receives a packet, the number of received packets, according to the type, will increase one. If the node forwards the received packet correctly, the number of forwarded packets will increase one. There are three scenarios that the number of received packets will not increase. Firstly, if the packet is dropped because of time to live (TTL), then the number of received packets should not increase. Secondly, if a node that receives a packet drops it due to overflow of buffers. Thirdly, a packet is dropped by a node because the state of wireless connection is bad. Considering these significant factors, we improve the accuracy of trust calculation.

SIMULATION RESULTS AND DISCUSSIONS

The proposed scheme is simulated on the Qualnet platform with the OLSRv2 protocol. In the simulations, the effectiveness of the scheme is evaluated in an insecure environment. We compare the performance of the proposed scheme with that of OLSRv2 without security mechanisms. 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. In this adversary mode, the proposed scheme is evaluated and compared with the original OLSRv2 protocol. We have simulated networks with different numbers of nodes. Fig. 4 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 in a 30-node MANET. The maximum velocity of each node is set from 0 to 10 m/s. The pause time is 30 seconds. 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, which are used to carry trust values; 5) *Routing load* is the ratio of the number of control packets transmitted by nodes to the number of data packets received successfully by destinations during the simulation.

TABLE II
SIMULATION PARAMETER



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

Although the number of packets received correctly decreases as long as the number of nodes increases, the performance of our scheme has a big improvement. The PDR declines in three schemes, the proposed scheme is apparently better than the existing scheme. In Fig. 4, we evaluate throughput in our scheme and the original. 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.

DOI 10.17148/IJARCCE.2015.4246

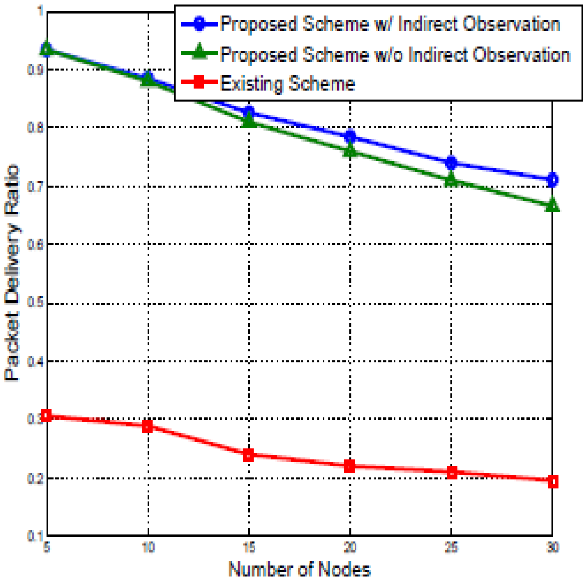


Fig. 4. Packet delivery ratio (PDR) versus the number of nodes in the network.

Conclusions and Future Work

In this paper, we proposed a unified trust management scheme that enhances the security of MANETs. Using recent advances in uncertain reasoning, Bayesian inference and Dempster-Shafer theory, we evaluate the trust values of observed nodes in MANETs. Misbehaviors 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. Future work will be made in order to reduce the time delay in MANETS while transmission.

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: distributed key management for security,” in *Proc. 2nd OLSR Workshop*, (Domaine de Voluceau, France), Dec. 2005.

BIOGRAHIES

Thamayanthi.M received her B.E degree in Computer Science and Engineering in Anna university Trichy, ariyalur campus in 2013, Tamilnadu, India. Now she is doing her Master in Engineering in St.Joseph's College of engineering and technology, Thanjavur, Tamilnadu, India. She has attended 5 national conferences, 3 international Journal and 2 international conference. She is interested in networks. Her future work is in ad hoc networks.

Arumai Ruban.J received his B.Sc in Physics and M.C.A in St. Joseph's College, Trichy, Bharathidasan University in 2007,2010 respectively, Tamilnadu, India. He has done his Master in Engineering in CSE, in Periyar Maniammai University, Thanjavur. He is working as an Assistant Professor in St.Joseph's College of engineering and technology, Thanjavur. He has handled various subjects and interested in Networks. He has attended 4 national conferences, 1 international Journal and 1 international conference.

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2015.4246