Trust Based Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments

M. Murugesan (Ahod/It) , R. Monica , A. Poornima, P. Pradeepa , D. M. Vijaya Lakshmi
Department of Information Technology
M.Kumarasamy College of Engineering,
Karur.

Abstract— **The distinctive features of mobile ad hoc networks (MANETs), including dynamic topology and open wireless medium, may lead MANETs suffering from many security vulnerabilities. In this paper, using recent advances in uncertain reasoning originated from artificial intelligence community, 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 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, also called secondhand information that is obtained from neighbor nodes of the 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. 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.**

Index Terms - MANETs, Security, Trust Management, Uncertain Reasoning.

I. INTRODUCTION

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 such as establishment environments

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 mobile phones. 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 secondhand 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, multi- agent 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 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 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

II. RELATED WORK

Trust-based security schemes are important detection-based methods in MANETs, which have been studied recently the trust value of a node based on direct observation is derived using Bayesian methodology. The authors of 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.

The Dempster-Shafer theory (DST) is regarded as a useful mechanism in uncertain reasoning and is widely used in expert systems and multi-agent systems. In, the Dempster-Shafer theory is used in sensor fusion. Intrusion detection systems apply the Dempster-Shafer theory to assess unreliable information from IDS sensors.

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. 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 are used to tackle the exceptions in automatic reasoning. In order to overcome the drawbacks of traditional rule-based systems, which are based on truth tables with no exceptions, probabilistic reasoning is proposed, in which the uncertainty of knowledge is considered and described as subsets of ”possible worlds.” 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 to evaluate trust of nodes by direct and indirect observation.

Trust based security systems are also studied in different network architectures, e.g., wireless sensor networks vehicular ad hoc networks (VANETs) cooperative wireless networks 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.

A. Definition and Properties of Trust

Trust has different meanings in different disciplines from Psychology to economy. The definition of trust in MANET 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. Due to the specific characteristics of MANETs, trust in MANETs has five basic properties: subjectivity, dynamicity, transitivity, asymmetry, and context dependency.

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.

TABLE I.
MAIN NOTATIONS

Notation	Definition
TAB	The total trust value that Node *A* gives Node *B*
TS *AB*	The trust value that Node *A* gives Node *B* based on direct observation of Node *A*
TN *AB*	The trust value that Node *A* gives Node *B* based on indirect observation of Node *A*
TD *AB*	The trust value that Node *A* gives Node *B* based on data packet
TC *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

B. 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 trustor needs to consider risk, 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. In direction observation trust, an observer estimates the trust of his one-hop neighbor 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. We denote T^S as a trust value from direct observation and can be calculated by Bayesian inference.

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. Although opinions of neighbors are introduced the method that simply takes arithmetic mean of all trust values is not sufficient to reflect the real meaning of other unreliable observers opinions because there are two situations that may disturb the effective evidence from neighbors: unreliable neighbors and unreliable observation. Unreliable neighbors themselves are suspects. Even though neighbors are trustworthy, they may also provide unreliable evidence due to observation conditions. The Dempster-Shafer theory 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. Combining the trust value T from direct observation and trust value T from indirect observation. We can get a more accurate trust value of a node in MANETs

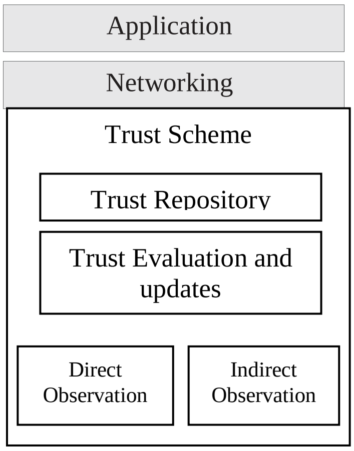
$$T = \lambda T^S + (1 - \lambda) T^N \qquad (11)$$

C. 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 $T^S_{AB} = \rho T^D_{AB} + (1-\rho) T^C_{AB}$, (2) where ρ ($0 \leq \rho \leq 1$) 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.

Fig. 1. The framework of the proposed scheme.



IV. TRUST EVALUATION WITH DIRECT OBSERVATION

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 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. As mentioned in the last section of trust model, the degree of belief is a random variable, denoted by Θ and

$0 \leq \theta \leq 1$. From Bayes' theorem, we can derive the following Formulation

$f(\theta,y|x)= p(x|\theta,y)f(\theta,y)\ 1\ 0\ p(x|\theta,y)f(\theta,y)d\theta$, (3)

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

$p(x|\theta,y)=y\ x\theta x(1-\theta)y-x$

We assume that the prior distribution, f(θ,y), follows Beta distribution,

$Beta(\theta;\alpha,\beta)= \theta\alpha-1(1-\theta)\beta-1 1\ 0\ \theta\alpha-1(1-\theta)\beta-1\ d\theta$, (5)

where $0\leq \theta \leq 1,\alpha>0,\beta>0$. Then we have

$f(\theta,y|x) \sim Beta(\alpha + x,\beta + y-x)$. (6)

The expectation of Beta distribution is

$E[\Theta] =\alpha\ \alpha + \beta$. (7)

Due to reproductivity of (6), the trust value is calculated iteratively. At the beginning, there is no observation. The prior distribution f(θ,y) is Beta(θ;1 ,1) at the beginning. Then we have

$En[\Theta] = \alpha n\ \alpha n + \beta n$, (8)

Where

$\alpha n = \alpha n-1 + xn-1,\beta n = \beta n-1 + yn-1 -xn-1,\alpha 0 = \beta 0 =1,n\in Z+$. Intuitively, this situation is explained that the trust value of a node is 0.5 at the beginning. That means the node is seemed as neutral when no history records behaviors is established. The value trust can be revised continuously through follow-up observation.

Past experience is also an important factor when trust values are calculated. Recent activities of a node can seriously affect the trust evaluation. Consider the case where a node has a good history of past experience, but it drops or modifies packets recently. In order to handle this, a windowing scheme is proposed. Using weighted evidence from observation is another method. Firstly, this can lower the trust of an attacker when it misbehaves. Secondly, the trust of the attack will not recover quickly even if it forwards a large number of packets correctly due to the impact of the punishment factor. This can help the proposed scheme distinguish the malicious node quickly and avoid them disrupting the normal traffic between benign nodes again. The punishment factor is inspired by our daily lives in human society, where a scandal can badly affect a person who has a good reputation. What's more, it is hard to quickly recover a good reputation. The factor of punishment makes the trust evaluation more realistic. The punishment factor, γ, in the formula of trust evaluation in (8) is described as follows:

$En[\Theta] = \alpha n\ \alpha n + \gamma\beta n$, (9)

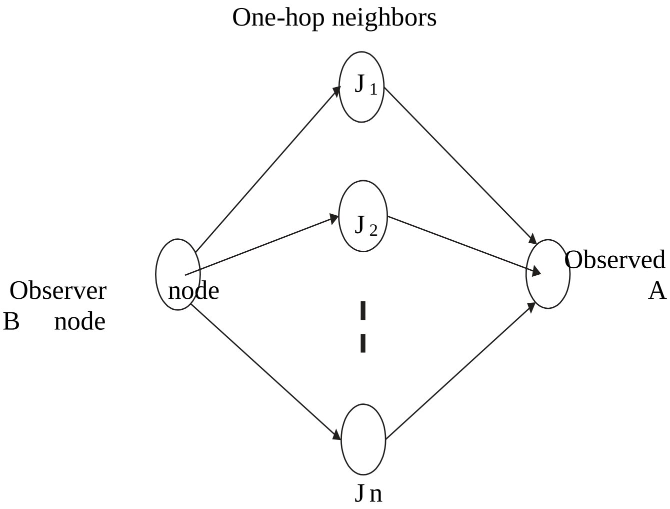
where $\gamma \geq 1$. As the value of γ becomes larger, the trust value declines more. This is because the punishment factor gives more weight to misbehavior. Based on this deduction, TS is defined as:

$TS = En[\Theta]$. (10)

V. 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.



A . Belief Function

In the Dempster-Shafer theory, a frame of discernment is a set of propositions that are mutually exclusive and exhaustive, which is denoted by Ω [29]. Based on the frame of discernment, the basic probability value of a focal set, Ai, is a function m2 Ω → [0,1], which satisfies following conditions: m(∅)=0; and Ai⊆Ω m(Ai)=1. For any subset B of the frame of discernment, the belief function is defined as

$$\text{Bel}\,(B) = \sum_{Ai\subseteq B} m(Ai) \qquad (11)$$

We designate two security states to a node, i.e., {trustworthy, untrustworthy. Therefore, the frame of discernment in the Dempster-Shafer theory Ω{trustworthy, untrustworthy}, which demonstrates that node B has two states: trustworthy and untrustworthy. Node A evaluates the trust value of node B through one-hop neighbors between them. One-hop neighbors of node B can provide evidence to a subset of Ω with hypothesis H, i.e., node B is trustworthy. The power set of our scenario, 2Ω, includes: ∅; hypothesis H = {trustworthy}; hypothesis H = {untrustworthy}; and hypothesis U =Ω, which means that the observed node B is either in the trustworthy state or untrustworthy state. Each one-hop neighbor gives evidence from its observation by assigning its beliefs over Ω. Each hypothesis is assigned a basic probability value m(H) between 0 and 1. In our scheme, the basic probability value can be obtained from direct observation. For example, the trust value of node j_1 is T^S_{Aj1}, from direct observation of node A to node j_1. If node j_1 believes that node B is trustworthy, then the basic probability value m_{j1} (H) is $T^S_{Aj1.}$. The basic probability value m_{j1} (H) is 0. From the definition of belief function, m_{j1} (U) is equal to $1-T^S_{Aj1}$. The formulae are as follows

$$m_{j1}\,(H) = T^S_{Aj1},$$
$$m_{j1}\,(H) = 0,$$
$$m_{j1}\,(U) = 1- T^S_{Aj1}, \qquad (12)$$

If node j1 believes that node B is untrustworthy, the formulae are as follows:

$$m_{j1}\,(H) = 0,$$
$$m_{j1}\,(H) = T^S_{Aj1,}$$
$$m_{j1}\,(U) = 1- T^S_{Aj1,} \qquad (13)$$

The belief function of each focal set can be obtained from (11). For example,

$$bel_{j1}\,(H) = m_{j1}\,(H),$$
$$bel_{j1}\,(H) = m_{j1}\,(H),$$
$$bel_{j1}\,(U) = m_{j1}\,(H) + m_{j1}\,(H) + m_{j1}\,(U). \ (14)$$

This means that from the testimony of node j_1, node A can derive whether or not node B is trustworthy based on the trust value of node j_1.

B. Dempster's Rule of Combining Belief Functions

Based on the above description of belief function, Dempster-Shafer theory combines multiple neighbor nodes' belief on the condition that evidence from different neighbor nodes is independent [25], [29]. Assuming that bel1(B) and bel2(B) are two belief functions over the same frame of discernment, Ω, the orthogonal sum of bel1(B) and bel2(B), bel(B), is defined as

$$\text{bel}\,(B) = \text{bel}_1\,(B) \oplus \text{bel}_2\,(B)$$
$$= \frac{\sum_{i,\,j,\,Ai\cap Aj\,=\,B} {}^{m}1\,(Ai)\;m2\,(Aj)}{\sum_{i,\,j,\,Ai\cap Aj\,\neq\,B} {}^{m}1\,(Ai)\;m2\,(Aj)}$$

Where Ai, A j ⊆ Ω. The order of the combination of belief functions does not affect the result value produced by Dempster' rule due to the commutatively of multiplication

In our scenario, we assume that there are one-hop neighbors beside node B as shown in Fig. 3. Therefore, the combined belief of node j1 and node j2 is calculated as follows

$m_{j1}\,(H) \oplus m_{j2}\,(H) = 1/K[m_{j1}\,(H)\, m_{j2}\,(H) + m_{j1}\,(H)\, m_{j2}\,(U) + m_{j1}\,(U)\, m_{j2}\,(H)],$

$m_{j1}\,(H) \oplus m_{j2}\,(H) = 1/K[m_{j1}\ (H)m_{j2}(H) + m_{j1}(H)m_{j2}(U) + m_{j1}(U)\, m_{j2}\,(H)],$

$m_{j1}\,(U) \oplus m_{j2}\,(U) = 1/K\ m_{j1}\,(U)\, m_{j2}\,(U), \qquad (16)$

Where

$K = m_{j1}(H)\, m_{j2}\,(H) + m_{j1}\,(H)\, m_{j2}\,(U) + m_{j1}\,(U)\, m_{j2}\,(U) + m_{j1}\,(U)\, m_{j2}(H) + m_{j1}\,(U)\, m_{j2}\,(H) + m_{j1}\,(H)\, m_{j2}\,(H) + m_{j1}\,(H)\, m_{j2}(U).$

For instance, assuming that

$m_{j1}\,(H) = 0.8,\ m_{j1}\,(H) = 0,\ m_{j1}\,(U) = 0.2,$

$m_{j2}\,(H) = 0\ .7,\ m_{j2}\,(H) =0,\ m_{j2}\,(U) = 0\ .3,$

Then we can obtain the result of combining two belief functions as follows:

bel (H) = 0.8∗0.7+0.8∗0.3+0.7∗0.2=0.94

bel (H) = 0 ∗0+0∗0.3+0∗0.2=0

bel (U) = 0 .2∗0.3=0 .06

That means from the result of combination, the trust value of node B from indirect observation is 0.94. Following the rule of combination of belief, we can combine more results from neighbor nodes. Based on the Dempster- Shafer theory, T^{N}_{AB} is defined as:

$T^{N}_{AB} = m_{j1}(H) \oplus m_{j2}(H) \ldots \oplus m_{jn}(H)$, (18)

Where $node_{ji,}$ $1 \leq i \leq n$, is an one-hop neighbor of node A and node B.

where T_{kiki+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 Trust 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 to avoid malicious attacks by enemies in battlefields.

VI. SECURE ROUTING BASED ON TRUST

The original OLSRv2 does not provide security measurements in the protocol. OLSRv2 assumes that every node cooperative and benevolent. However, this assumption is in appropriate 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 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 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. For other standard protocols, like AODV 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.

We assume that each node works in the promiscuous mode implemented by the MAC layer. We also assume that, in a time slot, the observed node (sender) does not move out of the transmission range. As the time of packets processing in a node is short, our assumptions are realistic in practical networks. This means that the observer can detect whether or not the neighboring node sends the received packets before the observed node moves out the transmission range.

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.

In this paper, we consider the condition that packets are dropped due to unreliable wireless connections. During the trust evaluation with direct observation, the scheme can remove the number of packets dropped by this condition (in Algorithm 1). We assume that there is a probability that packets are dropped because of unreliable wireless connections.

Algorithm 1 depicts the details of each iteration. Algorithm 2 describes that an observer node collects evidence from its one hops neighbors between 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 proactive routing protocols, such as OLSRv2, an observer node can obtain the information from its neighbor nodes periodically by control messages (e.g., HELLO and TC), which can be used to carry the trust values.

Algorithm 1 Trust Calculation with Direct Observation

```
1: if node A, which is an observer, finds that its one-hop neighbor, Node B that is a trustee, receives a packet then
2: the number of packets received increases one
```

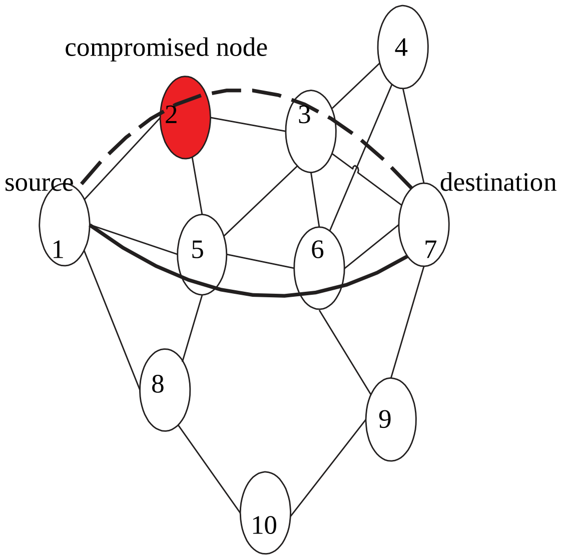
```
    if node A finds that node B forwards the packet successfully then
        the number of packets forwarded increases one
    else
        if TTL of the packet becomes zero or overflow of buffers in node B or the state of wireless connection of node B is bad then
            the number of packets 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 $TN$ to 0
    set $\lambda$ to 1
end if
```

Path using the Dijkstra's algorithm. To this end, we define the untrust worthy value between node *A* and node *B* as *UAB*, Which can be calculated as *UAB* = 1 − *TAB*. The sum of Untrustworthy values of a path is

$$U_{path} = \sum_{i=1}^{n-1} Ukiki + 1 \;\; = \sum_{i=1}^{n-1}(1 - Tkiki + 1) \quad (19)$$



VII. SIMULATION RESULTS AND DISCUSSIONS

The proposed scheme is simulated on the Qualnet platform with the OLSRv2 protocol. In the simulations, the effective- ness of the scheme is evaluated in an insecure environment. We compare the performance of the proposed scheme with that of OLSRv2 without security mechanisms.

A. Environment Settings

We randomly place nodes in the defined area has a pair of nodes as the source and destination with Constant 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. 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.

B. Performance Improvement

The original OLSRv2 and our scheme are evaluated in the simulations, where some nodes misbehave through dropping or modifying packets. In Fig. 5, we compare our scheme with and without indirect observation and original OLSRv2 in scenarios that a source node sends data packets to a destination node in the network, which includes nodes from 5 to 30. From Fig. 5, we can see that the proposed scheme has a much higher PDR than the existing scheme because the trust based routing calculation can detect the misbehavior of malicious nodes. The results also demonstrate that the proposed scheme with indirect observation has the highest PDR among these three schemes.

TABLE II SIMULATION PARAMETERS

Parameter	Value
Applicationprotocol	CBR
CBRtransmissiontime	1s to 100s
CBRtransmissioninterval	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

find that the PDR of three schemes decreases gradually when the number of nodes grows. This is because the collision of sending messages becomes more frequent as the number of nodes increases in the MANET. Although the PDR declines in three schemes, the proposed scheme is apparently better than the existing scheme. In Fig. 6, we evaluate throughput in our scheme and the original one. 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. Fig. 5 and Fig. 6 both reveal that the trust based routing algorithm can improve the performance of OLSRv2. Fig. 7 and Fig. 8 show the impact of node mobility in a 30-node MANET.

We can observe that, as the node velocity increases, PDR and throughput decrease gradually. This is because the higher speed of a node may increase the probability of packets lost. Nevertheless, the proposed scheme has better performance than the existing one. 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 a30-node MANET environment. The basic parameter is the same as above. Fig. 9 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 2 malicious nodes. we can see that the proposed scheme is affected deeply by the number of malicious nodes. Compared to the proposed scheme, the existing scheme has a very low throughput even if the number of malicious nodes is very small. , 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 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.

C. Cost

The cost of security enhancement in OLSRv2 mainly includes the increased average end-to-end delay and overhead of messages that are used to carry trust values of nodes. Fig. 10 shows that the proposed scheme has a slightly higher average end-to-end delay than the existing scheme in the malicious environment. In Fig. 11, we can see that, as the node velocity increases, 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, higher security is guaranteed in the proposed scheme. Compared to 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 OLSRv2 protocol. Since the metric link value is introduced in OLSRv2, one new address block TLV, which occupies 12 bytes, is added to the message format described in Section VI. Fig. 12 shows how much the overhead of messages is imported compared to the original version of OLSRv2. Because trust values are embedded in the HELLO messages and TC messages, there is no more messages 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 Fig. 13. This is because, when the number of nodes increases, the total message becomes large. Then the 12-byte overhead is trivial compared to the size of messages. In Fig. 14, the results demonstrate that the proposed scheme 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 load of the existing and proposed schemes climb up due to the nature of proactive routing protocol: periodical generation of control messages in every node.

VIII. CONCLUSION

In this paper, we proposed a unified trust management scheme that enhances the security of MANETs. Using re- cent 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, indirect observation from one-hop neighbors 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: distributed 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.