TAODV: A Trusted AODV Routing Protocol for Mobile Ad Hoc Networks

Abstract

In this paper, we design and formulate a novel trust-based routing protocol for secure transactions, such as military and disaster relief operations, in mobile ad hoc networks (MANETs). The innovative approach is employing the idea of a trust model in the network layer of MANET so as to achieve security in mobile ad hoc networks cost-effectively. A salient feature of this approach is that, by establishing formal trust relationships among nodes, computation-intensive digital signature authorization and verification are not required for most of the secure transactions in the MANET, and hence the computation cost of the whole network can be considerably reduced. Specifically, in our trust model, trust among nodes is represented by opinion, a term derived from the subjective logic. The values of opinions are updated during a routing information exchange process. If a node performs healthy behaviors, its credibility from the viewpoints of other nodes is increased; otherwise, the credibility will be decreased, and this node will be eventually denied by the whole network. We also devise an effective recommendation mechanism to exchange the trust information among nodes. The performance of our protocol is evaluated through analyses and simulations. The results demonstrate that the whole MANET system can be maintained at a satisfactory security level with reasonable short convergence time and significant lower computation overheads. More importantly, the security level can be easily customized to meet the diverse demands from applications over ad hoc networks.

Keywords: Trust model, Secure routing protocol, Ad hoc networks, Wireless security, MANET

Contents

1 Introduction

A mobile ad hoc network (MANET) [5][22] is a kind of wireless network without centralized administration or fixed network infrastructure, in which nodes communicate over relatively bandwidth constrained wireless links and perform routing discovery and routing maintenance in a self-organized way. The topology of the MANET may change uncertainly and rapidly due to the high mobility of the independent mobile nodes, and because of the network decentralization, each node in the MANET will act as a router to discover the topology and maintain the network connectivity. Unlike the wired networks, the MANET must take into account many factors such as wireless link quality, power limitation, multiuser interference and so on. The routing determination is also more difficult in the MANET. Nowadays the MANET enables many promising applications in the areas of emergancy operations, disaster relief efforts, and military battlefield networks. These kinds of applications often comprise lots of independent mobile nodes and demand establishing efficient, reliable and dynamic network communications rapidly. Especially for the millitary environment, preservation of security, latency, reliablity, intentional jamming, and recovery from failure are significant concerns. On the other hand, with some characteristics such as openness, mobility, dynamic topology and protocol weaknesses, MANETs are prone to be unstable and attemptable. Consequently, the security issue of MANETs are becoming an urgent requirement.

Many security schemes from different aspects of MANETs have been proposed in recent years, such as secure routing protocols [11], [31], [30], [10], [25] and secure key management solutions [33], [18], [12], [4], [19]. However, most of them assume centralized units or trusted third-parties to issue digital certificates, which actually destroy the self-organization nature of MANETs. And by requiring nodes to perform digital signature authentication all the time, these solutions often bring huge computation overheads. Our solution is, on the other hand, a secure routing protocol which employs the idea of a trust model so that it can avoid introducing large overheads and influencing the self-organization nature of MANETs.

In this paper, we apply the trust model into security solutions of MANETs. Our trust model is derived and modified from subjective logic [16], [15], [14], which qualitatively defines the representation, calculation, and combination of trust. Trust models have found security applications in e-commerce, peer-to-peer networks, and some other distributed systems [17] [2][29][1][26]. In recent years, some research work was conducted to apply trust models into the security solutions of MANETs [9][7]. However, there are no concrete and applicable designs proposed for routing protocol security solutions in MANETs, to the best of our knowledge.

We design our secure routing protocol based on Ad hoc On-demand Distance Vector (AODV) routing protocol [24]. The new protocol, called TAODV (Trusted AODV), has several salient features: (1) Nodes perform trusted routing behaviors mainly according to the trust relationships among them; (2) A

node who performs malicious behaviors will eventually be detected and denied to the whole network; (3) System performance is improved by avoiding generating and verifying digital signatures at every routing hop. The idea of the trust model can also be applied into other routing protocols of MANETs, such as DSR [13], DSDV [23] and so on.

The remaining of this paper is organized as follows. Some background overviews about AODV routing protocol, several securiy solutions for MANETs, and subjective logic are introduced in Section 2. In Section 3, we present the system framework and network assumptions for the TAODV protocol. Our trust model are described in Section **??**. We illustrate our TAODV protocol details including routing discovery and maintenance procedures as well as trust recommendation and updating algorithms in Section 5. Performance and security analyses are presented in Section 6 and Section 7. Finally we conclude the paper in Section 8.

2 Background

2.1 Routing Protocols for MANETs

There are several routing protocols have been proposed for mobile ad hoc networks, such as AODV, DSR, DSDV and so on. We will introduce AODV routing protocol, on which our trusted protocol is based.

2.1.1 AODV

AODV (Ad hoc On-demand Distance Vector) routing protocol [24] is one of the most popular routing protocols for MANETs. On-demand is a major characteristic of AODV, which means that a node only performs routing behaviors when it wants to discover or check route paths towards other nodes. This will greatly increase the efficiency of routing processes. Routing discovery and routing maintenance are two basic operations in AODV protocol.

Routing discovery happens when a node wants to communicate with a destination while it obtain no proper route entry for that destination. In this situation, this source node (originator) will broadcast an RREQ (Routing REQuest) message to all its neighbors. Each neighbor who receives this RREQ will check in its own routing table if it contains the route entry for that destination. If not, it will set up a reverse path towards the originator of RREQ and rebroadcast this routing request. Any node which receives this RREQ will generate a RREP (Routing REPly) message if it either has a fresh enough route to satisfy the request or is itself the destination. Then this intermediate or destination node will generate an RREP message and unicast it to the next hop toward the originator of the RREQ, as indicated by the routing entry for that originator. When a node receives an RREP message, it first updates some fields of the route table and the routing reply, and then forwards it to the next hop towards the originator. In this

way, this RREP will ultimately reach the source node and a bidirectional route path will be established between the source and destination. Thus, these two ends can communicate with each other using the route path just set up.

Routing maintenance is performed through two ways. One is that a node may positively offer connectivity information by broadcasting hello messages locally so that its neighbors can determine the connectivity by listening for the hello packets. The other way is that a node can maintain local connectivity to its next hops using some link or network layer mechanisms, such as the detection mechanism of IEEE802.11 MAC (Media Access Control) protocol.

Our secure routing protocol is based on AODV and is called TAODV (Trusted AODV), which concerns trust information when performing routing discovery and routing maintenance.

2.2 Secure Routing Protocols for MANET

Although the existing routing protocols are effective and efficient to a certain extent, they are designed without security consideration. The following sections are several secure routing protocols proposed especially for original routing protocols of MANETs.

2.2.1 SAODV

Secure AODV (SAODV) proposed by M.G.Zapata and N. Asokan is based on AODV routing protocol. Two mechanisms are used to secure the AODV messages: hash chains to secure the hop count information which is the only mutable information in the messages; and digital signatures to authenticate the non-mutable fields of the messages. The information relative to the hash chains and the signatures is transmitted with the AODV message as an extension message.

SAODV uses hash chains to authenticate the hop count of RREQ and RREP messages in such a way that allows every intermediate or destiantion node that receives the message to verify that the hop count has not been decremented by an attacker. A hash chain is formed by applying a one-way hash function repeatedly to a seed.

Digital signatures are used in SAODV to protect the integrity of the non-mutable data in RREQ and RREP messages. That means that they sign everything but the Hop_Count of the AODV message and the Hash from the SAODV extension. The main problem in applying digital signatures is that a RREP message generated by an intermediate node should be able to sign it on behalf of the final destination. SAODV offers Double Signature Extension to solve this problem, which is that every time a node generates a RREQ message, it also includes the RREP flags, the prefix size and the signature of RREP.

When a node receive a RREQ, it first verifies the signature. Only if the signature is verified, will it store the route. If the RREQ has a Double Signature Extension, then the node will also store the signature for the RREP and the lifetime in the route entry. An intermediate node will reply to a RREQ

with a RREP only if it fulfills the AODV's requirements to do so and the node has the corresponding signature and old lifetime to put into the Signature and Old Lifetime fields of the RREP Double Signature Extension. Otherwise, it will rebroadcast the RREQ.

When a RREQ is received by the destination itself, it will reply with a RREP only if it fulfills the AODV's requirements to do so. This RREP will be sent with a RREP Single Signature Extension.

When a node receives a RREP, it first verifies the signature before creating or updating a route to that host. Only if the signature is verified, will it store the route with the signature of the RREP and the lifetime.

SAODV can prevent several attacks commonly performed to AODV routing protocol. However, SAODV's signatures require a processing power that might be excessive for certain kinds of ad hoc scenarios.

2.2.2 Ariadne

Ariadne [11] is an on-demand secure routing protocol based on DSR which withstands node compromise and relies on symmetric cryptography. It designs the Ariadne protocol in three stages. First it enables the target to verify the authenticity of the ROUTE REQUEST by using a MAC with a key shared between the initiator and the target; then each intermediate node can employs three alternative techniques, the TESLA protocol, digital signatures, and standard MACs, to perform data (node list) authentication in ROUTE REQUEST and ROUTE REPLY; and finally it presents an per-hop hashing mechanism to guarantee that no node can be removed from the node list in the REQUEST.

TESLA is a broadcast authentication protocol for authenticating routing messages. It adds a Message Authentication Code (MAC) computed with a shared key to a message, which can provide secure authentication in point-to-point communication. TESLA achieves asymmetry from clock synchronization and delayed key disclosure. When Ariadne performs Route Discovery using TESLA broadcast authentication, it assume that every node has a TESLA one-way key chain.

A ROUTE REQUEST in Ariadne extend original DSR Route Request to eight fields: *ROUTE REQUEST, initiator, target, id, time interval, hash chain, node list*, and *MAC list*. The *time interval* is the TESLA time interval at the pessimistic expected arrival time to the target, accounting for clock skew.

When any node A receives a ROUTE REQUEST for which it is not the target, besides checking the receive repetition, the nodes checks whether the *time interval* is valid: that time interval must not be too far in the future, and the key corresponding to it must not have been disclosed yet. If the time interval is not valid, the node discards the packet. Otherwise, the node modifies the REQUEST by appending its own address, A, to the node list in the REQUEST, replacing the hash chain field with $H[A, hashchain]$, and appending a MAC of the entire REQUEST to the MAC list. The node uses the TESLA key KAi to compute the MAC, where i is the index for the time interval specified in the REQUEST. Finally, the

node rebroadcasts the modified REQUEST, as in DSR.

When the target node receives the ROUTE REQUEST, it checks the validity of the REQUEST by determining that the keys from the time interval specified have not been disclosed yet, and that the hash chain field is correct. If the target node determines that the REQUEST is valid, it returns a ROUTE REPLY to the initiator, containing eight fields: *ROUTE REPLY, target, initiator, time interval, node list, MAC list, target MAC,* and *key list*. The *target MAC* is set to a MAC computed on the preceding fields in the REPLY with the key $KDS?$. The ROUTE REPLY is then returned to the initiator of the REQUEST along the source route.

A node forwarding a ROUTE REPLY waits until it is able to disclose its key from the time interval specified; it then appends its key from that time interval to the *key list* field in the REPLY and forwards the packet according to the source route indicated in the packet.

When the initiator receives a ROUTE REPLY, it verifies that each key in the key list is valid, that the *target MAC* is valid, and that each MAC in the *MAC list* is valid. If all of these tests succeed, the node accepts the ROUTE REPLY; otherwise, it discards it.

Ariadne is efficient because it uses only symmetric cryptographic primitives. But it requires clock synchronization to achieve ”asymmetry”, which is argued that it is an unrealistic requirement for ad hoc networks.

2.3 Key Managements for secure MANET

Other than implementing security in the network layer of MANET, some key management schemes have been proposed above the network layer to provide cryptography solutions to MANETs. Traditional key management solutions commonly employ a trusted third-party or centralized servers, which violate the nature of MANETs. And recently researchers have proposed several self-organized or semi-self-organized key managements schemes. We will present several of them in the following.

2.3.1 Self-Organized Public-Key Management for MANETs [4]

This work proposed a fully self-organized public-key management scheme that does not rely on trusted authority or fixed server. Each user in this mechanism is her own authority domain and issues public key certificates to other users. Each user also keeps a local certificate repository containing a subset of certificates issued by herself and certificates selected according to an appropriate algorithm that issued by other users. Key authentication is performed via a chain of certificates. When user u wants to verify the authenticity of the public key of user v, they merge their local certificate repositories, and u tries to find an appropriate certificate chain from u to v in the merged repository.

In order to thwart attacks by dishonest users, they extended their scheme with authentication metrics. A set of criteria are proposed for the design of the local repository construction algorithms, based on

which they consider a tradeoff between the size of the local repositories of the users and the communication load/key usage.

This public-key management system is realized in a fully self-organized, yet scalable way. However, it only provide probabilistic guarantees.

2.3.2 Providing robust and ubiquitous security support for MANET [18]

This work describes a solution that supports ubiquitous security services for mobile hosts, scales to network size, and is robust against break-ins. It distributes the certification authority functions through a threshold secret sharing mechanism, in which each entity holds a secret share and multiple entities in a local neighborhood jointly provide complete services. Each secret share is updated periodically to resist gradual break-ins.

The system is based on public key infrastructure and the system CA (Certification Authority) has a key pair $\{SK, PK\}$, where SK, Secret Key, is shared among the network entities and PK, Public Key, is well-known to the whole system. Each entity vi holds a secret share Pvi, and any K of such secret share holders can collectively function as the role of CA. The SK is not visible by any component of the network except at the system bootstrapping phase. Each secret share Pvi can be obtained during system bootstrapping phase or through a self-initialization service. A self-initialization algorithm is devised to securely deliver the secret share to a uninitialized entity by a local coalition of K secret share holders.

When an entity requests for certification service, a local coalition of K secret share holders to the requester a partial certificate that is signed by a value SKi which is directly derived from the secret share Pvi. once the requester locally collects K such partial certificates, it combined them together and obtains its complete certificate that is signed by SK.

In this system, no adversary group having less than K collaborative adversaries can forge a valid certificate so that it can tolerate up to $K - 1$ break-ins from each adversary group. It has K-out-of-N security.

2.4 Subjective Logic

Subjective logic is a kind of trust model which was proposed by A. Josang [16], [15], [14]. It is "a logic which operates on subjective beliefs about the world, and uses the term opinion to denote the representation of a subjective belief" [16]. The trust between two entities is then represented by *opinion*. An opinion can be interpreted as a probability measure containing secondary uncertainty.

In MANET, nodes move with high mobility and may experience long distance in space among each other. A node may be uncertain about another node's trustworthiness because it does not collect enough evidences. This uncertainty is a common phenomenon, therefore we need a model to represent such uncertainty accordingly. Traditional probability model, which is also used in some trust models, cannot

express uncertainty. While in subjective logic, an opinion consists of belief, disbelief and also uncertainty, which gracefully meets our demands. Subjective logic also provides a mapping method to transform trust representation between the evidence space and the opinion space.

Our trust model used in TAODV is then derived and modified from the subjective logic and is more applicable for the instance of MANET. In the subjective logic, an opinion includes four elements. The fourth one is *relative atomicity* which can be used in combination operations of the opinion. We omit this last parameter in order to simplify our implementation and make our trust representation more meaningful. In addition, we substantiate the definition of the opinion by changing opinions about the 'TRUE' or 'FALSE' state of a proposition to opinions about a real node entity's trustworthiness. The evidences we use in our trust model are collected through the successful or failed state when nodes perform routing actions or communications with other nodes.

3 Overview of the Trusted AODV (TAODV)

3.1 Network Model and Assumptions

In this work, we make some assumptions and establish the network model of TAODV. We also argue why we focus our security solution on routing protocol in the network layer.

We do not concern the security problem introduced by the instability of physical layer or link layer, and only assume that: (1) Each node in the network has the ability to recover all of its neighbors; (2) Each node in the network can broadcast some essential messages to its neighbors with high reliability; (3) Each node in the network possesses a unique ID that can be distinguished from others.

In the TAODV, we also assume that the system is equipped with some monitor mechanisms or intrusion detection units either in the network layer or the application layer so that one node can observe the behaviors of its one-hop neighbors. These mechanisms have been proposed in some previous work, such as intrusion detection system in [32] and watchdog technique in [20].

A self-organized key management mechanism, such as threshold secret share solutions in [4] or [18], can cooperate with the TAODV. These solutions provide secure ways to issue public key certificates which can be used for the generation and verification of digital signatures during the initialization of the TAODV or a newly joined node. In these cases, certificates are issued corporately by several nodes, which is consistent with the ways of updating trust relationships in the TAODV and with our motivation of keeping any operation self-organized. Furthermore, the TAODV and the self-organized key management scheme can benefit from each other. The selection of trusted certificate issuers in key management can refer to the trust information among nodes; and the digital signature extension is a good supplement to perform trusted routing operations.

We achieve security in the network layer of MANET because of such considerations. Nodes in

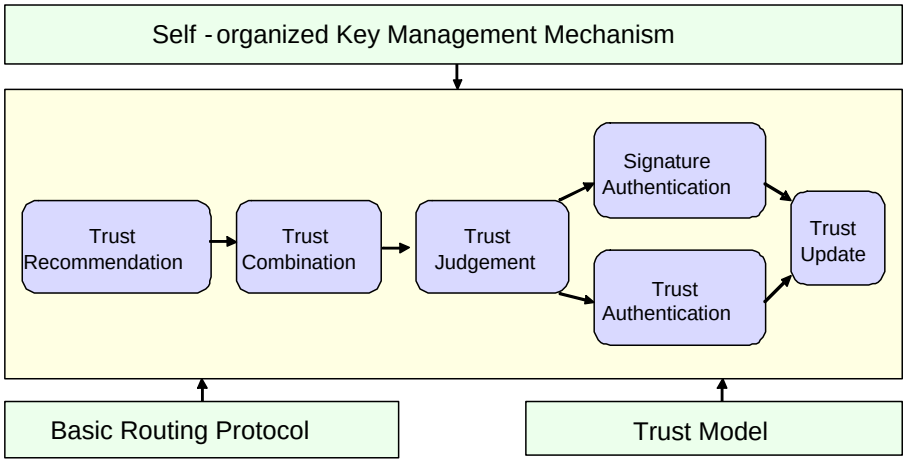

Figure 1. Framework of the Trusted AODV (TAODV)

MANETs usually have high mobility and also high invalidity, which make it difficult to maintain secure end-to-end connections. In such case, it is easier and more reasonable to implement security hop by hop in the routing layer. And we are also not interested in the link layer security.

3.2 Framework of the Trusted AODV

There are mainly four modules in this trusted MANET: *basic routing protocol*, *trust model*, *trusted routing protocol*, and *self-organized key management mechanism*, which is illustrated in Figure 1. In our work, we mainly focus on the module of *trust model* and *trusted routing protocol*. The module of *trusted routing protocol* contains such parts as trust recommendation, trust combination, trust judging, signature authentication routing, trusted authentication routing, and trust updating. We will explain the designs of these modules and parts detailedly in Section 4 and 5.

Our trusted routing protocol and trust model can be applied to different routing protocols in MANET and we will take AODV routing protocol for example to illustrate our ideas.

4 Trust Model for TAODV

4.1 Trust Representation

Our trust model is an extension of the original trust model in subjective logic (See Section 2.4). Here *opinion* is modified to a 3-dimensional metric and is defined as follows:

Definition 1 (Opinion). *Let* $\omega_B^A = (b_B^A, d_B^A, u_B^A)$ *denote any node* A*'s opinion about any node* B*'s trustworthiness in a MANET, where the first, second and third component correspond to belief, disbelief*

and uncertainty, respectively. These three elements satisfy:

$$b_B^A + d_B^A + u_B^A = 1 \tag{1}$$

In this definition, belief means the probability of a node B can be trusted by a node A, and disbelief means the probability of B cannot be trusted by A. Then uncertainty u_B^A fills the void in the absence of both belief and disbelief, and sum of these three elements is 1.

4.2 Mapping between the Evidence and Opinion Spaces

A node in MANET will collect and record all the positive and negative evidences about other nodes' trustworthiness, which will be explained in detail in Section 5.4. With these evidences we can obtain the opinion value by applying the following mapping equation which is derived from [16].

Definition 2 (Mapping). *Let $\omega_B^A = (b_B^A, d_B^A, u_B^A)$ be node A's opinion about node B's trustworthiness in a MANET, and let p and n respectively be the positive and negative evidences collected by node A about node B's trustworthiness, then ω_B^A can be expressed as a function of p and n according to:*

$$\begin{cases} b_B^A &= \frac{p}{p+n+2} \\ d_B^A &= \frac{n}{p+n+2} \\ u_B^A &= \frac{2}{p+n+2} \end{cases} , where \quad u_B^A \neq 0. \tag{2}$$

4.3 Trust Combination

In our trust model, a node will collect all its neighbors' opinions about another node and combine them together using combination operations. In this way, the node can make a relatively objective judgment about another node's trustworthiness even in case several nodes are lying. The followings are two combination operations nodes may adopt: Discounting Combination and Consensus Combination.

4.3.1 Discounting Combination

Let's consider such a situation: Node A wants to know C's trustworthiness, then node B gives its opinion about C. Assuming A already has an opinion about B. Then A will combine the two opinions: A to B, B to C to obtain a *recommendation opinion* A to C. Discounting combination is for this purpose.

Definition 3 (Discounting Combination). *Let A, B and C be three nodes where $\omega_B^A = (b_B^A, d_B^A, u_B^A)$ is A'S opinion about B's trustworthiness, and $\omega_C^B = (b_C^B, d_C^B, u_C^B)$ is B's opinion about C's trustworthiness. Let $\omega_C^{AB} = (b_C^{AB}, d_C^{AB}, u_C^{AB})$ be the opinion such that*

$$\begin{cases} b_C^{AB} &= b_B^A b_C^B \\ d_C^{AB} &= b_B^A d_C^B \\ u_C^{AB} &= d_B^A + u_B^A + b_B^A u_C^B \end{cases} \tag{3}$$

ω_C^{AB} is called the discounting of ω_C^B by ω_B^A which expresses A's opinion about C as a result of B's advice to A. By using the symbol '$\otimes$' to designate this operator, we define $\omega_C^{AB} \equiv \omega_B^A \otimes \omega_C^B$.

The discounting combination can be used along a recommendation path.

4.3.2 Consensus Combination

Different nodes may have different, even contrary opinions about one node. To combine these opinions together to get a relative objective evaluation about that node's trustworthiness, we may use Consensus combination.

Definition 4 (Consensus Combination). *Let $\omega_C^A = (b_C^A, d_C^A, u_C^A)$ and $\omega_C^B = (b_C^B, d_C^B, u_C^B)$ be opinions respectively held by nodes A and B about node C's trustworthiness. Let $\omega_C^{A,B} = (b_C^{A,B}, d_C^{A,B}, u_C^{A,B})$ be the opinion such that*

$$\begin{cases} b_C^{A,B} &= (b_C^A u_C^B + b_C^B u_C^A)/k \\ d_C^{A,B} &= (d_C^A u_C^B + d_C^B u_C^A)/k \\ u_C^{A,B} &= (u_C^A u_C^B)/k \end{cases} \tag{4}$$

where k=$u_C^A + u_C^B - 2u_C^A u_C^B$ such that $k \neq 0$, Then $\omega_C^{A,B}$ is called the consensus between ω_C^A and ω_C^B, representing an imaginary node $[A, B]$'s opinion about C's trustworthiness, as if it represented both A and B. By using the symbol '$\otimes$' to designate this operator, we define $\omega_C^{A,B} \equiv \omega_C^A \oplus \omega_C^B$.

The consensus combination can reduce the uncertainty of one's opinion.

5 Routing Operations in TAODV

In this section, we first illustrate the trust recommendation mechanism used in TAODV. Then we define some rules for a node in TAODV to obey make routing decisions according to opinion values. Also some policies are derived for a node to update its opinions towards others. After that, we describe our TAODV protocol extensions and several scenarios of trusted routing discovery operations in details.

5.1 Trust Recommendation

Existing trust models seldom concern the exchange of trust information. However, it is necessary to design an trust information exchange mechanism when applying the trust models into network applications. In TAODV, we devise an efficient trust recommendation mechanism. There are two types of messages used in the recommendation procedures: Trust Request Message (TREQ), and Trust Reply Message (TREP). The formats of TREQ and TREP are shown in Figure 2 and Figure 3.

When a node A wants to know another node B's latest trustworthiness, it will broadcast an TREQ message to its neighbors. This TREQ message follows the above format with the *Type* field set to 0 and

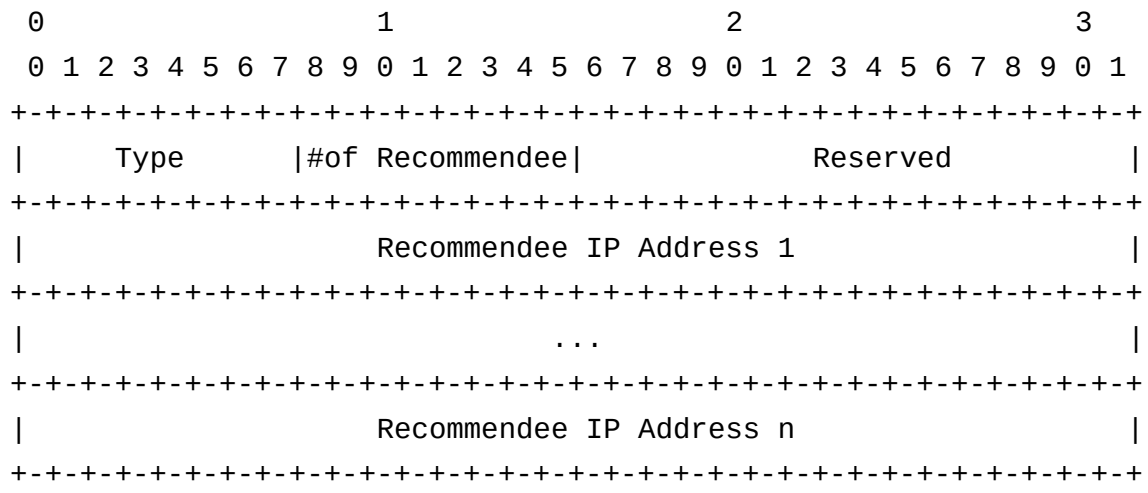

Figure 2. Trust Request (TREQ) Message Format

Table 1. Criteria for Judging Trustworthiness

belief	disbelief	uncertainty	Actions
		> 0.5	Request and verify digital signature
	> 0.5		Distrust a node for an expire time
> 0.5			Trust a node and continue routing
≤ 0.5	≤ 0.5	≤ 0.5	Request and verify digital signature

the *Recommendee* field filled with the IP address of node B. If one of A's neighbors C receives the TREQ message C will reply with an TREP message. The *Type* field of this TREP is set to 1 and the *Opinion* field is filled with the opinion values from C to B. Note that, in this recommendation protocol, a node can request or reply several opinion values of different nodes simutaneously in one TREQ or TREP packet. In this way, we can efficiently exchange trust information without introducing much packets overhead.

5.2 Trust Judgement

Before describing the process of trusted routing discovery and maintenance in detail, we predefine some trust judging rules here and in Table 1. These rules tell a node how to perform the corresponding operation according to the values in its opinion about another node.

- In node A's opinion towards node B's trustworthiness, if the first component *belief* of opinion ω_B^A is larger than 0.5, A will trust B and continue to perform routing behaviors related to B or begin data packets transmission.

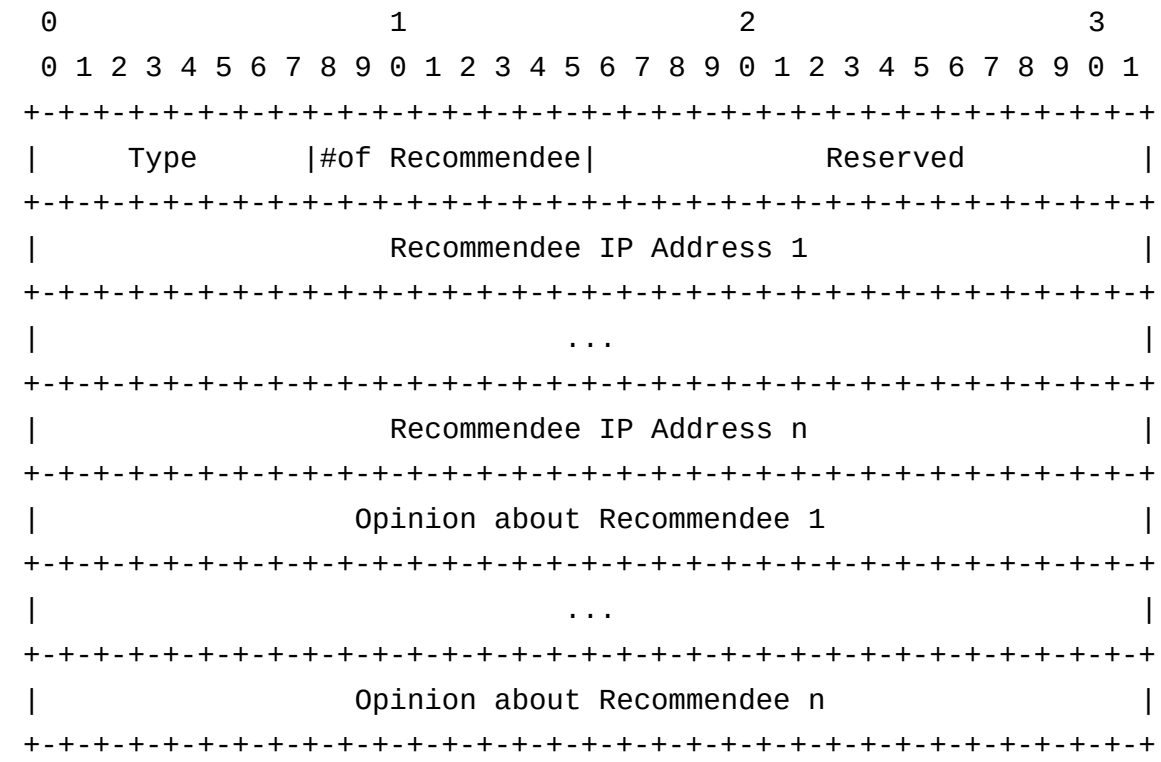

Figure 3. Trust Reply (TREP) Message Format

- In node A's opinion towards node B's trustworthiness, if the second component *disbelief* of opinion ω_B^A is larger than 0.5, A will not trust B and will refuse to perform routing behaviors related to B. Accordingly the route entry for B in A's route table will be disabled and deleted after an expire time.

- In node A's opinion towards node B's trustworthiness, if the third component *uncertainty* of opinion ω_B^A is larger than 0.5, A will request and verify B's digital signature.

- In node A's opinion towards node B's trustworthiness, if the three components of opinion ω_B^A are all smaller than or equal to 0.5, A will also request and verify B's digital signature.

- If node B has no route entry in node A's route table, A's opinion about B is initialized as (0,0,1).

5.3 Trust Update

Opinions among nodes change dynamically with the increase of successful or failed communication events. When and how to update trust opinions among nodes follows some policies as follows:

- Each time a node A has performed a successful communication with another node B, including

DestinationIP	···	Next Hop	···	Lifetime	···	State	Expiry	**Positive Events**	**Negative Events**	**Opinion**

Figure 4. ModifiedExtended Route Table with Trust Information

forwarding route requests or replies normally, generating route requests or route replies normally, etc., B's successful events in A's route table will be increased by 1.

- Each time a node A has performed a failed communication with another node B, including forwarding route requests or replies abnormally, generating route requests or route replies abnormally, authenticating itself incorrectly, and so on, B's failed events in A's route table will be increased by 1.

- Each time when the field of the successful or failed events changes, the corresponding value of opinion will be recalculated using Equation 2, which is a mapping function from the evidence space to the opinion space.

- If node B's route entry has been deleted from node A's route table because of expiry, the opinion ω_B^A will be set back to the initial value (0,0,1).

5.4 Route Table Extension

We add three new fields into each node's route table: *positive events*, *negative events* and *opinion*. *Positive events* are the successful communication times between two nodes. Similarly *negative events* are the failed communication ones. *Opinion* means this node's belief towards another node's trustworthiness as defined before. The value of opinion can be calculated according to Equation 2. One node's route table can be illustrated by Figure 4, where some fields are omitted for highlighting the main parts.

5.5 Routing Messages Extensions

We extend basic AODV routing messages by appending some trust information fields. Two main types of extended messages are TRREQ (Trusted Routing REQuest) and TRREP (Trusted Routing REPly). Figure 5 and 6 show the formats of these messages.

In trusted routing discovery procedures, every routing request and reply carries trust information, including opinions towards originator nodes S and destination node D, which will be empolyed to calculate the credibility of S and D. When a node is required to provide its certificate information, it will fill the fields of trust information with its own signature, as proposed by some traditional security solutions for MANETs.

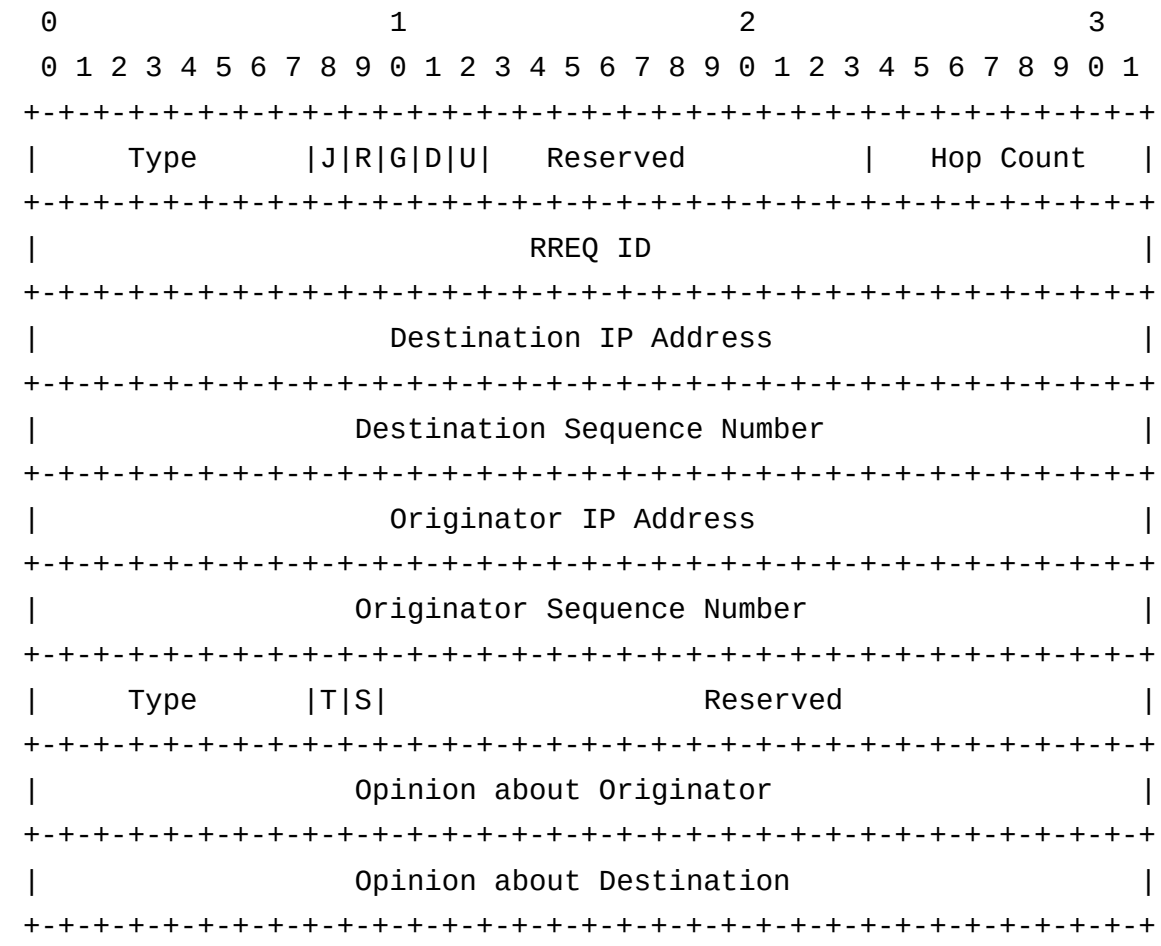

Figure 5. Trusted Routing Request (TRREQ) Message Format

An RERR message, which is sent by a node to report route invalidation in original AODV procedure, now will also be used for informing the worst trust warning. That is, when a node A cannot pass the critical signature verification, its opinion from the viewpoint of another node B will be set to $(0, 1, 0)$, which means total disbelif, and B will broadcast an RERR msg. Every node which receives this message will verify B's trustworthiness then perform corresponding update.

5.6 Trusted Routing Discovery

In this section, we will formulate the general trusted routing discovery procedure and describe it with an example shown in Figure 7. In this figure, the route path from the originator S to the destination D is uncovered. S will generate an TRREQ message to discover a route path to D. Node N is an intermediate node along this path, and node $N1$ to $N4$ are its four neighbors. When N receives the re-broadcast TRREQ message from $N1$, it will perform such operations as illustrated in Algorithm 1.

Algorithm 1 General Procedure of Node N in Performing Trusted Routing Discovery

Receive an TRREQ(S,D) or an TRREP(S,D) from $N1$;

/*Verify the trustworthiness of $N1$*/
Broadcast TREQ(N1) to request the opinions from N's neighbors to $N1$;
Reveive opinions from N's neighbors: ω_{N1}^{N2}, ω_{N1}^{N3}, ω_{N1}^{N4};

Combine these opinions together and get a latest ω_{N1}^{N};

/*Check each component in ω_{N1}^{N}, and judge the next step using the criteria in Table 1*/
if uncertainty> 0.5 **then**
  Request and verify $N1$'s certificate;

else if disbelief> 0.5 **then**
  Update the $N1$ entry in the route table;
  Distrust $N1$ for an expiry time;

else if belief> 0.5 **then**
  Calculate ω_{S}^{N}, and ω_{D}^{N} using the lastest ω_{N1}^{N};
  Update the S and D entries in the route table;
  Trust $N1$ and re-broadcast TRREQ/TRREP;

else
  /*Do not have much confidence about $N1$'s trustworthiness.*/
  Request and verify $N1$'s certificate, by default;
end if

if Succeed in verifying $N1$'s certificate **then**
  Calculate ω_{S}^{N}, and ω_{D}^{N} using the lastest ω_{N1}^{N};
  Update the S and D entries in the route table;
  Trust $N1$ and re-broadcast TRREQ/TRREP;

else
  /*N1 doesn't pass the certificate verification*/
  Set ω_{N1}^{N} to $(0, 1, 0)$;
  Broadcast TRERR(N1) to N's neighbors;
  Update the $N1$ entry in the route table;
  Distrust $N1$;
end if

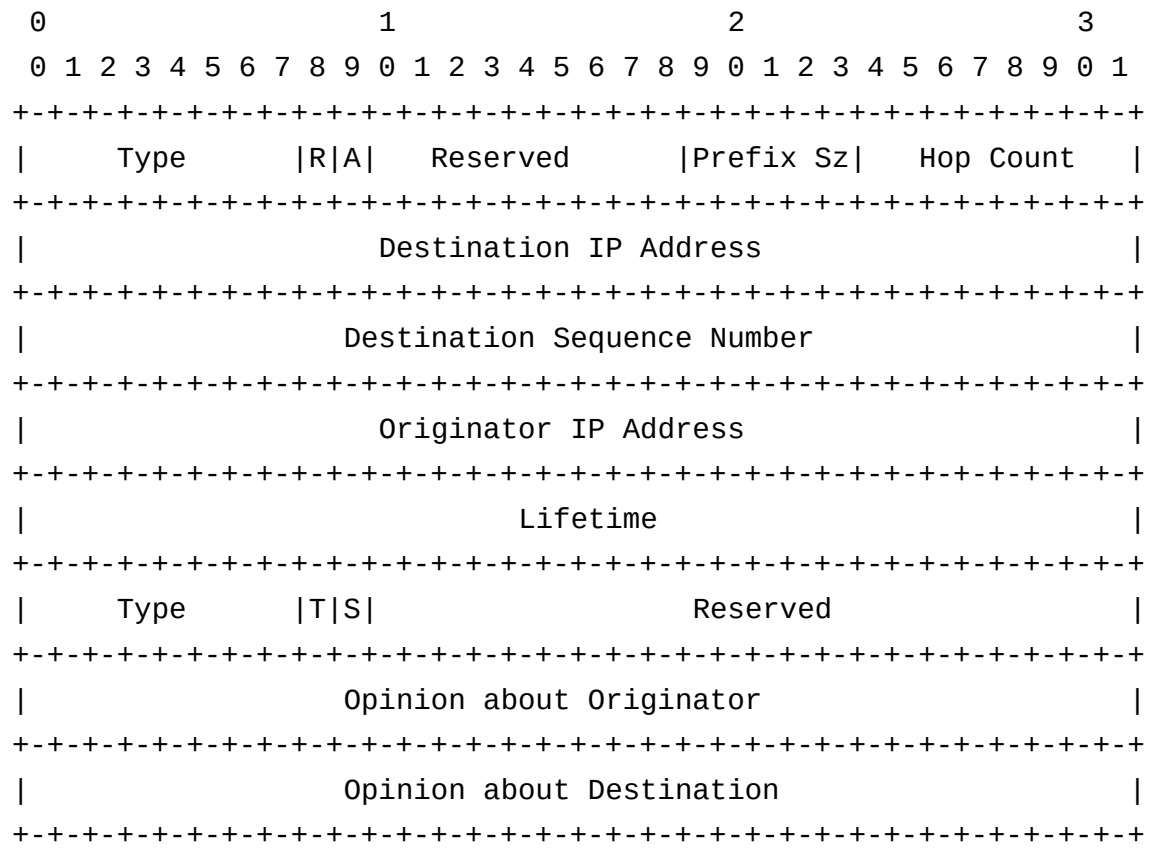

Figure 6. Trusted Routing Reply (TRREP) Message Format

Specifically, in the above algorithm, node N wants to verify node $N1$'s trustworthiness. It then collects its neighbors' recommendations towards $N1$ and combines these opinions together using the combination equations in Section 4.3. Node N originally has opinions about $N1$, $N2$, $N3$, and $N4$: ω_{N1}^{N}, ω_{N2}^{N}, ω_{N3}^{N} and ω_{N4}^{N}. The opinions it receives from its neighbors are: ω_{N1}^{N2}, ω_{N1}^{N3}, and ω_{N1}^{N4}. We can illustrate the trust recommendation relationships using Figure 8, where the arrows denote opinion directions. First, $N1$ calculates the following opinions using Equation 3:

$$\begin{aligned} \omega_{N1}^{NN2} &= \omega_{N2}^{N} \otimes \omega_{N1}^{N2} \\ \omega_{N1}^{NN3} &= \omega_{N3}^{N} \otimes \omega_{N1}^{N3} \\ \omega_{N1}^{NN4} &= \omega_{N4}^{N} \otimes \omega_{N1}^{N4} \end{aligned}$$

Second, the new opinion ω_{N1}^{N} can be combined as follows:

$$\omega_{N1}^{N} = \omega_{N1}^{N(N2,N3,N4)}$$

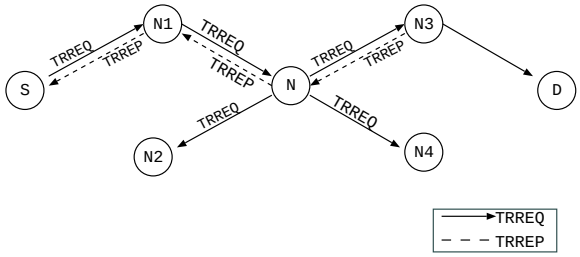

Figure 7. An Example for Trusted Routing Discovery

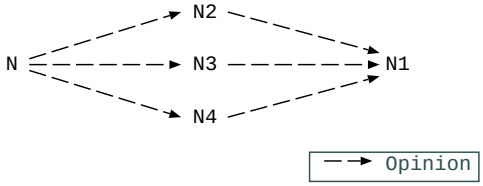

Figure 8. An Example for Trust Combination

$$
\begin{aligned}
&= \omega_{N1}^{NN2} \oplus \omega_{N1}^{NN3} \oplus \omega_{N1}^{NN4} \\
&= (\omega_{N2}^{N} \otimes \omega_{N1}^{N2}) \oplus (\omega_{N3}^{N} \otimes \omega_{N1}^{N3}) \oplus (\omega_{N4}^{N} \otimes \omega_{N1}^{N4})
\end{aligned}
$$

5.7 Initiation of a TAODV MANET

Let us consider a simple MANET which only contains 3 nodes: A, B and C. The topology of this minimal MANET is shown in Figure 9. In this figure, node A has only one neighbor: B, node B has two neighbors: A and C, and node C also has one neighbor: B. Node A and B are not neighborhood. At the beginning, there is no entry in each node's route table, and as said in Section 5.4, the initial value of each node's opinion towards one another is $(0, 0, 1)$. Now suppose node A wants to discover a route path to node C. The processes of node A, B, and C are listed below.

1. A broadcasts an RREQ requesting route path to C, then begins waiting for an RREP from its neighbor B.

2. B receives the RREQ from A, it then:

   (a) Checks a route to C and opinion ω_A^B and ω_C^B. Because it is the very beginning of this MANET, there should be no route for C and $\omega_A^B = \omega_C^B = (0, 0, 1)$.

   (b) Authenticates A because $u_A^B > 0.5$. B requests A's certificate and verifies it. If A passes, the successful events is increased by 1, and the new opinion $\omega_A^B = (0.33, 0, 0.67)$. B will then authenticate C following the previous steps. If A can not pass, the failed events is increased by 1, then the new opinion is $\omega_A^B = (0, 0.33, 0.67)$. B will not forward the RREQ.

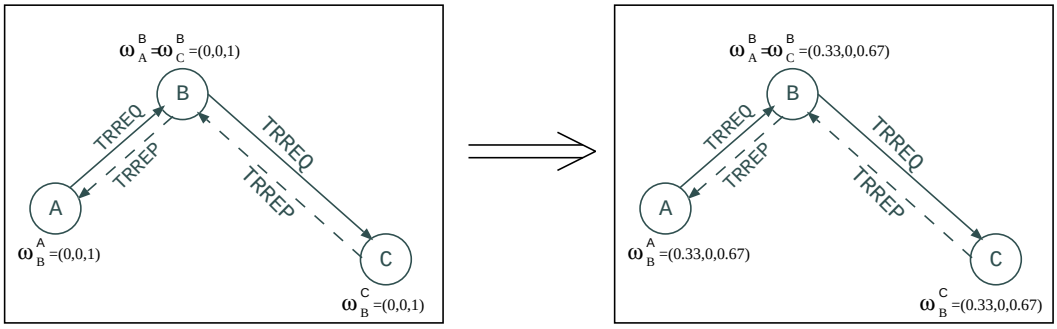

Figure 9. Initialization for TAODV

(c) If C has also been authorized, B's route table will be updated and B will re-broadcast the RREQ. If C can not pass the authentication, B will not forward this RREQ. The opinion ω_C^B will be re-calculated accordingly.

3. C receives the re-broadcasted RREQ from B. It will also check opinion ω_B^C and B's authenticity. If B passes, C will generate an RREP back to B and update its route table. If not, C will drop the RREQ and update ω_B^C.

5.8 Trusted Routing Maintenance

The procedure of trusted routing maintenance is very similar to that of trusted routing discovery. Nodes will also use trust information to judge other nodes' trustworthiness. We omit the detailed algorithms here.

6 Analysis

First, we evaluate the computation overheads of one node in a TAODV MANET when given a certain routing traffic volumn and compare the cost with a general secure routing solution which employs digital signature authentication. In TAODV, the computation cost of one node can be measured from two aspects. One is the cost of each trust update operation. The other is the number of trust update operations when given a certain number of total routing packets.

In TAODV, the cost of trust combination is $O(v)$, where v is the number of a node's neighbors. Each trust combination needs a constant number of multiplications, where the length of factor is 16 bit. Hence the overall cost of each trust combination requires $O(16^2 v)$ bit operations. For security solutions employing digital signature authentication, we use the RSA signature scheme for example to measure the computation cost of signature generation and verification. explain the computation overheads in signature authentication solutions. In general when using a $2k$-bit RSA signature, the generation of

signature requires $O(k^3)$ bit operations and the verification requires $O(k^2)$ bit operations, where k is recommended at least to be 1024 bits for most security applications [21]. In the TAODV, the cost of trust combination satisfies $O(v)$, where v is the number of a node's neighbors. To do one time trust combination, a constant multiplication times is needed with 16-bit factors. Overall the trust combination requires $O(16^2 v)$ bit operations. We can conclude from this aspect that the TAODV achieves better computation performance compared to pure signature authentication solutions.

On the other hand, we compare the times of performing digital authentication and trust updating when given a certain traffic volumn. The digital authentication schemes usually need to generate or verify signature for every routing message. While in the TAODV protocol, with the help of expiry time of trust values, the trust updating times can be significantly reduced. Let us assume that the total number of routing packets propagated in the whole network is n, the average packet transmission interval is t, and the average expiry time of a trust value is e. Obiviously the times of performing digital authentication is a constant value n because the generation or verification is required for each packet. The times of performing trust updating can be obtained by Equation 5 in the following. The policy for updating trust used in this equation is that we combine periodical update and on-demand update together. When nodes in the MANET all have high mobility, the routing messages are sent in a high-frequency way. If the average packet sending interval t is smaller than the average expiry time, we update trust values periodically. When the nodes in the MANET stay in more stable positions, the average packet sending interval t is long. If the average packet interval value t is larger than the expiry time, we update the trust in an on-demand way.

$$U = \begin{cases} \lfloor \frac{nt}{e} \rfloor & , \quad t < e \\ n & , \quad t \geq e \end{cases} \tag{5}$$

We now assume that the total number of routing packets are 600 and the average expiry time is 10s, then we can draw a figure according to Equation 5 in Figure **??**. It can be concluded that when the network has a high throughput it is quite efficient using TAODV routing protocol. For those solutions that perform signature authentication not only for routing packets but also for data packets, the computation overheads will be largely reduced because we do not perform trust updating when transmitting data packets if we have established trust routes between the source nodes and the destinations.

From security point of view, our design will detect nodes' misbehavior finally and reduce the harms to the minimum extent. When a good node is compromised and becomes a bad one, its misbehavior will be detected by its neighbors. Then with the help of trust update algorithm, the opinions from the other nodes to this node will be updated shortly. Thus this node will be denied access to the network. Similarly, a previous bad node can become a good one if the attacker leaves or the underlying links are recovered. In this situation, our design allows this node's opinion from other nodes' points of view to be

Table 2. Parameters for TAODV Simulation Study

Number of Nodes	50
Node Velocity Range	0-20 m/s
Simulation Field	1500 m * 300 m
Source-Destination Pairs	20
Source Packet Rate	4 pkts/s
Source Data Packet Size	512 bytes
Physical Link Bandwidth	2 Mbps
Nominal Radio Range	250 m

updated from $(0, 1, 0)$ to $(0, 0, 1)$ after a period of expiry time.

From flexibility point of view, the TAODV gives each node flexibility to define its own opinion threshold. The default opinion threshold is 0.5, which can be increased by a node to maintain a hight security level and also can be decreased to meet demands of some applications.

7 Simulations

7.1 Simulation Environment

We performed a set of simulations based on *ns-2* [8] with extensions for mobile wireless networks which is developed by Monarch reserach group in CMU. This extended simulator has good support for simulating complete wireless network protocol model from physical and data link layer, MAC layer, routing layer to application layer. Lucent's WaveLAN [6] [27] is used as the radio model with 2 Mb/sec bit-rate and 250 meters radio range. The MAC layer is implemented according to IEEE802.11 Distributed Coordination Function (DCF).

To evaluate the performance of TAODV without attackers, the basic movement and traffic models in our simulation are as follows. 50 nodes moved in a 1500m * 300m field according to *random waypoint* model [3] with a velocity uniformly distributed between 0 and 20 m/s. Each of the node moves from a random location to a randomly chosen destination initially. On arriving, the node will stop for a *pause time* then move to next random destination. By varying *pause time* we achieve different network mobility. This process repeates in each simulation run of 900 seconds. To simulate communication traffic, 20 source-destination pairs are chosen and randomly distributed over the network. The traffic source sends 4 data packets of 512 bytes per second using CBR (Constant Bit-Rate). The parameters are listed in Table 2.

7.2 Misbehaving Model

To evaluate the TAODV with internal malicious or abnormal nodes, we provide a misbehaving model for simulation. The misbehavior we focus on in our simulation is *no forwarding* behaviors which commonly occur in mobile ad hoc networks caused by either internal attackers or invalid nodes. *No forwarding* means that a node participates in a wireless network but does not forward any routing operation packets, such as ROUTE REQUEST and ROUTE REPLY messages, or performs normal routing operations but silently drops certain data packets.

We vary the number of misbehaving nodes among 50 nodes from 0 to 20, so that the max percentage of misbehaving nodes in the simulated network is 40%, which is an extremely high ratio in real network environment. These nodes are chosen randomly by Tcl's [28] built-in pseudo-random number generator and keeps dropping routing packets or data packets for a period of 200 seconds.

7.3 Metrics

We compute the following metrics to evaluate our TAODV.

1. *Packet Delivery Ratio*: The ratio of the number of data packets received at the destination to the number of those originated at the application layer by the CBR traffic sources.

2. *Packets Overhead*: The total number of routing operation packets transmitted in the simulation run. Those packets across multi-hops are counted as number of hops transmissions.

3. *Byte Overhead*: The total number of transmission bytes of routing packets, counting method is as above.

4. *Average end-to-end delay of data packets*: End-to-end delay represents the application level latency between the source and the destination application level. In our simulation, the end-to-end delay takes into account not only the routing discovery latency, the queueing and buffering delays at the interface queue, the data propagation and transmission time, and the retransmission delays at the MAC layer, but also the computation delays caused by computation and verification of trust values or signatures.

5. *Normalized routing load*: The number of routing packets needed to deliver a data packet to the destination.

6. *False Report Ratio*: The ratio of the good nodes reported to be misbehaved among all the nodes.

7. *Omission Report Ratio*: The ratio of the misbehaving nodes not reported among all the misbehaving nodes.

8 Conclusion and Future work

This paper is the first to apply the idea of a trust model in subjective logic into the security solutions of MANETs. The trust and trust relationship among nodes can be represented, calculated and combined using an item *opinion*. In our TAODV routing protocol, nodes can cooperate together to obtain an objective opinion about another node's trustworthiness. They can also perform trusted routing behaviors according to the trust relationship among them. With an opinion threshold, nodes can flexibly choose whether and how to perform cryptographic operations. Therefore, the computational overheads are reduced without the need of requesting and verifying certificates at every routing operation. Our trusted AODV routing protocol is a more light-weighted but more flexible security solution than other cryptography and authentication designs.

In the future we will optimize our trusted routing algorithm and establish some fast response mechanisms when malicious behaviors of attackers are detected. We will also work at applying the trust model into other applications (e.g., key management) and other routing protocols of the MANET (e.g., DSR and DSDV). A detailed simulation evaluation will be conducted in terms of message overhead, security analysis, and tolerance to mobile attackers.

References

[1] A. Abdul-Rahman and S. Halles. A distributed trust model. In *Proceedings of New Security Paradigms Workshop '97*, pages 48–60, 1997.

[2] T. Beth, M. Borcherding, and B. Klein. Valuation of trust in open networks. In *Proceedings of the European Symposium on Research in Computer Security*, pages 3–18, Brighton, UK, 1994. Springer-Verlag.

[3] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Proceeding of the ACM/IEEE Mobile Computing and Networking (MobiCom)*, pages 85–97, 1998. http://citeseer.nj.nec.com/broch98performance.html.

[4] S. Capkun, L. Buttyan, and J.-P. Hubaux. Self-organized public-key management for mobile ad hoc networks. In *Proceedings of ACM Workshop on Wireless Security (WiSe '02)*, Atlanta, USA, September 2002. http://citeseer.nj.nec.com/capkun02selforganized.html.

[5] S. Corson and J. Macker. Mobile ad hoc networking (manet): Routing protocol performance issues and evaluation considerations (rfc2501), January 1999. http://www.ietf.org/rfc/rfc2501.txt.

[6] D. Eckhardt and P. Steenkiste. Measurement and analysis of the error characteristics of an in-building wireless network. In *Proceedings of the ACM SIGCOMM'96*, pages 243–254, October 1996.

[7] L. Eschenauer, V. D. Gligor, and J. Baras. On trust establishment in mobile ad-hoc networks. In *Proceedings of the Security Protocols Workshop*, Cambridge, UK, April 2002. Springer-Verlag. http://citeseer.nj.nec.com/eschenauer02trust.html.

[8] K. Fall and K. Varadhan, editors. *ns notes and documentation*. 2003. http://www.isi.edu/nsnam/ns/doc/index.html.

[9] E. Gray, J.-M. Seigneur, Y. Chen, and C. Jensen. Trust propagation in small worlds. In *Proceedings of the 1st International Conference on Trust Management*, 2002. http://citeseer.nj.nec.com/575876.html.

[10] Y.-C. Hu, D. B. Johnson, and A. Perrig. Sead: Secure effi cient distance vector routing in mobile wireless ad hoc networks. In *Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02)*, pages 3–13, June 2002. http://citeseer.nj.nec.com/hu02sead.html.

[11] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom '02)*, Atlanta, USA, September 2002. http://citeseer.nj.nec.com/article/hu02ariadne.html.

[12] J.-P. Hubaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In *Proceedings of ACM Symposium on Mobile Ad Hoc Networking and Computingi (MobiHoc '01)*, 2001.

[13] D. B. Johnson and D. A. Maltz. Dynamic source routing protocol in ad hoc wireless networks. In T. Imielinski and H. Korth, editors, *Mobile Computing*, chapter 5, pages 153–181. Kluwer Academic Publishers, Boston, USA, 1996.

[14] A. Josang. Prospectives for modelling trust in information security. In *Proceedings of Australasian Conference on Information Security and Privacy*, pages 2–13, 1997. http://citeseer.nj.nec.com/josang97prospectives.html.

[15] A. Josang. A subjective metric of authentication. In *Proceedings of European Symposium on Research in Computer Security (ESORICS '98)*. LNCS, Springer-Verlag, 1998. http://citeseer.nj.nec.com/josang98subjective.html.

[16] A. Josang. A logic for uncertain probabilities. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 9(3):279–311, 2001.

[17] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molna. The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th International World Wide Web Conference (WWW '03)*, Budapest, Hungary, 2003.

[18] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks. In *Proceedings of IEEE ICNP '01*, 2001.

[19] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang. Self-securing ad hoc wireless networks. In *Proceedings of IEEE ISCC '02*, 2002.

[20] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of Mobile Computing and Networking (MobiCom '00))*, pages 255–265, 2000. http://citeseer.nj.nec.com/marti00mitigating.html.

[21] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, fi fth edition, 1996.

[22] C. E. Perkins, editor. *Ad Hoc Networking*. Boston: Addison-Wesley, 2001.

[23] C. E. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. In *Proceedings of the ACM Conference on Communications Architectures, Protocols and Applications (SIGCOMM '94)*, pages 234–244, London, UK, 1994. ACM Press. http://doi.acm.org/10.1145/190314.190336.

[24] C. E. Perkins and E. M. Royer. Ad hoc on-demand distance vector routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, 1999. http://citeseer.nj.nec.com/article/perkins97adhoc.html.

[25] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer. A secure routing protocol for ad hoc networks. citeseer.nj.nec.com/551839.html.

[26] Y. Teng, V. V. Phoha, and B. Choi. Design of trust metrics based on dempster-shafer theory. http://citeseer.nj.nec.com/461538.html.

[27] B. Tuch. Development of wavelan, and ism band wireless lan. *AT&T Technical Journal*, 72(4):27–33, July/August 1993.

[28] B. Welch, K. Jones, and with Jeff Hobbs. *Practical Programming in Tcl and Tk*. Prentice Hall, 2003.

[29] R. Yahalom, B. Klein, and T. Beth. Trust relationships in secure systems - a distributed authentication perspective. In *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy (RSP '93)*, pages 150–164, 1993.

[30] H. Yang, X. Meng, and S. Lu. Self-organized network-layer security in mobile ad hoc networks. In *Proceedings of ACM Workshop on Wireless Security (WiSe'02)*, Atlanta, USA, September 2002.

[31] M. G. Zapata and N. Asokan. Securing ad hoc routing protocols. In *Proceedings of ACM Workshop on Wireless Security (WiSe '02)*, pages 1–10, Atlanta, USA, September 2002. ACM Press. http://doi.acm.org/10.1145/570681.570682.

[32] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In *Proceedings of the 6th ACM Annual International Conference on Mobile Computing and Networking (MobiCom '00)*, pages 275–283, Boston, Massachusetts, USA, 2000. ACM Press. http://doi.acm.org/10.1145/345910.345958.

[33] L. Zhou and Z. J. Haas. Securing ad hoc networks. *Journal of IEEE Networks*, 13(6):24–30, 1999.