A Trust Model Based Routing Protocol for Secure Ad Hoc Networks

Xiaoqi Li, Michael R. Lyu, and Jiangchuan Liu
Department of Computer Science and Engineering
The Chinese University of Hong Kong
Shatin, N.T., Hong Kong
+852-2609-8344
{xqli, lyu, ljc}@cse.cuhk.edu.hk

Abstract— Security issues have been emphasized when mobile ad hoc networks (MANETs) are employed into military and aerospace fields. In this paper, we design a novel secure routing protocol for MANETs. This protocol TAODV (Trusted AODV) extends the widely used AODV (Ad hoc On-demand Distance Vector) routing protocol and employs the idea of a trust model to protect routing behaviors in the network layer of MANETs. In the TAODV, trust among nodes is represented by *opinion*, which is an item derived from subjective logic. The opinions are dynamic and updated frequently as our protocol specification: If one node performs normal communications, its opinion from other nodes' points of view can be increased; otherwise, if one node performs some malicious behaviors, it will be ultimately denied by the whole network. A trust recommendation mechanism is also designed to exchange trust information among nodes. The salient feature of TAODV is that using trust relationships among nodes, there is no need for a node to request and verify certificates all the time. This greatly reduces the computation overheads. Meanwhile, with neighbors' trust recommendations, a node can make objective judgement about another node's trustworthiness to maintain the whole system at a certain security level.

TABLE OF CONTENTS

1. INTRODUCTION

A mobile ad hoc network (MANET) [1][2] is a kind of wireless network without centralized administration or fixed network infrastructure, in which nodes perform routing discovery and routing maintenance in a self-organized way. Nowadays MANET enables many promising applications in the areas of aerospace and military. Due to some of its characteristics such as openness, mobility, dynamic topology and protocol weaknesses, MANETs are prone to be unstable and vulnerable. Consequently, their security issues become more urgent requirements and it is more difficult to design and implement security solutions for MANETs than for wired networks. Many security schemes from different aspects of MANETs have been proposed, such as secure routing protocols [3], [4], [5], [6], [7] and secure key management solutions [8], [9], [10], [11], [12]. 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 request and verify digital signatures 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 the security solutions of MANETs. Our trust model is derived and modified from subjective logic [13], [14], [15], 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 [16] [17][18][19][20]. In recent years, some research work is conducted to apply trust models into the security solutions of MANETs [21][22]. However, there are no concrete and applicable designs proposed for the security of routing protocols 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 [23]. 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 requesting and verifying certificates at every routing step. The idea of the trust model can also be applied into other routing protocols of MANETs, such as DSR [24], DSDV [25] and so on.

The remaining of this paper is organized as follows. Some background overviews about subjective logic and AODV routing protocol are introduced in Section 2. In Section 3,

0-7803-8155-6/04/$17.00/©2004 IEEE
IEEEAC paper # 1150

we present the system framework and network assumptions for the TAODV protocol. Our trust model are described in Section 4. 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. Finally we conclude the paper in Section 7.

2. BACKGROUND

Subjective Logic

Subjective logic is a kind of trust model which was proposed by A. Josang [13], [14], [15]. 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" [13]. 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 evidence. 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.

Ad hoc On-demand Distance Vector Routing Protocol

Ad hoc On-demand Distance Vector (AODV) routing protocol [23] 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 routing 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.

3. OVERVIEW OF THE TRUSTED AODV (TAODV)

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.

Mobile nodes in MANETs often communicate with one another through an error-prone, bandwidth-limited, and insecure wireless channel. We do not concern the security problem introduced by the instability of physical layer or link layer. We 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, the physical network interface address for example, 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 neigh-

bors. These mechanisms have been proposed in some previous work, such as intrusion detection system in [26] and watchdog technique in [27].

Another kind of secure routing protocol which uses cryptography technologies is recommended to take effect before nodes in the TAODV establish trust relationships among one another. [3] and [4] are the latest security schemes for securing MANET, which employ cryptography technologies. We assume that the keys and certificates needed by these cryptographic technologies have been obtained through some key management procedures before the node performs routing behaviors.

In the network layer, a new node model is designed as the basis of our trust model. Some new fields are added into a node's routing table to store its opinion about other nodes' trustworthiness and to record the positive and negative evidences when it performs routing with others. By embedding our trust model into the routing layer of MANET, we can save the consuming time without the trouble of maintaining the expire time, valid state, etc. which is important in the situation of high node mobility and invalidity. Also because of this reason, it is hard to design secure solutions in the transport layer, which is an end-to-end communication mechanism.

Framework of the Trusted AODV

There are mainly three modules in the whole TAODV system: basic AODV routing protocol, trust model, and trusted AODV routing protocol. Based on our trust model, the TAODV routing protocol contains such procedures as trust recommendation, trust combination, trust judging, cryptographic routing behaviors, trusted routing behaviors, and trust updating. The structure and relationship among these components are shown in Figure 1. The general procedure for establishing trust relationships among nodes and for performing routing discovery is described as follows.

Let us first imagine the beginning of an ad hoc network which contains a few nodes. Each node's opinion towards one another initially is (0,0,1), which means that the node does not trust or distrust another node but it is only uncertain about another node's trustworthiness. Suppose node A wants to discover a route path to B. Because the uncertainty element in A's opinion towards others is larger than or equal to 0.5, which means that A is not sure whether it should believe or disbelieve any other nodes, A will use the cryptographic schemes as proposed in SAODV [4] or some other schemes to perform routing discovery operations. After some successful or failed communications, A will change its opinions about other nodes gradually using the trust updating algorithm. The uncertainty elements in its opinions about other nodes will be mostly less than 0.5 after a period of time. By means of this procedure, each node in this MANET will form more certain opinions towards other nodes eventually after this period of initial time.

Once the trust relationship is established among most of the nodes in this ad hoc network, these nodes can use our trusted routing protocol which is based our trust model to perform routing operations. Note that the trust relationships among nodes are not symmetric. That is, if node A totally trust B, B may not have the same opinion about A's trustworthiness. Node A now will use the trust recommendation protocol to exchange trust information about a node, B, from its neighbors, then use the trust combination algorithm to combine all the recommendation opinions together and calculate a new option towards B. The sequent routing discovery and maintenance operations will follow the specifications of our trusted routing protocol. Note that the situation that one node first joins a MANET can be handled in the same way as at the beginning of this whole network.

In this framework, the establishment of trust relationships among nodes and the discovery of route paths are all performed in a self-organized way, which is achieved by the cooperation of different nodes to exchange information and to obtain agreements without any third-party's interventions.

4. Trust Model for TAODV

Trust Representation

Our trust model is an extension of the original trust model in subjective logic which is introduced in Section 2. In our trust model, *opinion* is 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.

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. With these evidences we can obtain the opinion value by applying the following mapping equation which is derived from [13].

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:*

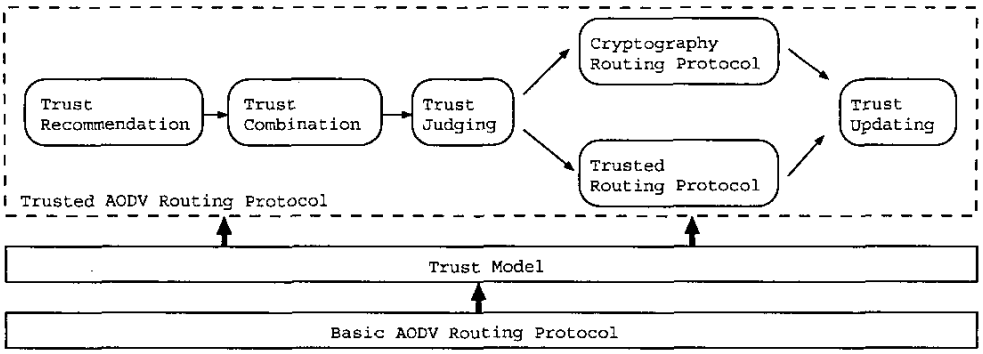


Figure 1. Framework of the Trusted AODV (TAODV)

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

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.

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*

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

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.

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*

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

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

Node Model

We add three new fields into each node's original routing 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 Formula 2. These three fields are the main factors when performing trusted routing. One node's routing table can be illustrated by Figure 2, where some fields are omitted for highlighting the main parts.

DestinationIP	DestinationSeq	...	HopCount	...	Lifetime	Positive Events	Negative Events	Opinion

Figure 2. Modified Routing Table with Trust Information

Trust Judging Rules

Before describing the process of trusted routing discovery and maintenance in detail, we predefine some trust judging rules here and in Table 1.

(1) 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 related to B.

(2) 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 performing routing related to B. Accordingly the route entry for B in A's routing table will be disabled and deleted after an expire time.

(3) 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 B's digital signature whenever A has interaction (or relationship) with B.

(4) 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 request B's digital signature whenever A has interaction (or relationship) with B.

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

Trust Updating Policies

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

(1) Each time a node A has performed a successful communication with another node B, including forwarding route requests or replies normally, generating route requests or route replies normally, etc., B's successful events in A's routing table will be increased by 1.

(2) 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 routing table will be increased by 1.

(3) Each time when the field of the successful or failed events changes, the corresponding value of opinion will be recalculated using Equation 2 from the evidence space to the opinion space.

(4) If node B's route entry has been deleted from node A's route table because of expiry, or there is no B's route entry from the beginning, the opinion ω_B^A will be set to (0,0,1).

Trust Recommendation

Existing trust models seldom concern the exchange of trust information. However, it is necessary to design an information exchange mechanism when applying the trust models into network applications. In our trust recommendation protocol, there are three types of messages: Trust Request Message (TREQ), Trust Reply Message (TREP), and Trust Warning Message (TWARN). Nodes who issue TREQ messages are called *Requestor*. Those who reply TREP messages are called *Recommender*. The recommendation target nodes are called *Recommendee*. Any node may be a *Requestor*, a *Recommender*, or a *Recommendee*. These three types of messages share a common message structure, which is shown in Figure 3.

When a node wants to know another node's new trustworthiness, it will issue an TREQ message to its neighbors. TREQ message uses the above structure and leaves the fields of *Recommender*, *Opinion* and *Expiry* empty. The *Type* field is set to 0. Nodes which receive the TREQ message will reply with an TREP message with the *Type* field set to 1. When a node believes that another node has become malicious or unreliable, it will broadcast a TWARN message with the *Type* set to 2 to its neighbors.

Trusted Routing Discovery

We take AODV for example to illustrate how to perform trusted routing discovery using the idea of our trust model.

Scenario I: Beginning 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 4.

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 C are not neighbors. At the beginning, there is no entry in each node's routing table, and as said in Section 5, 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:

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

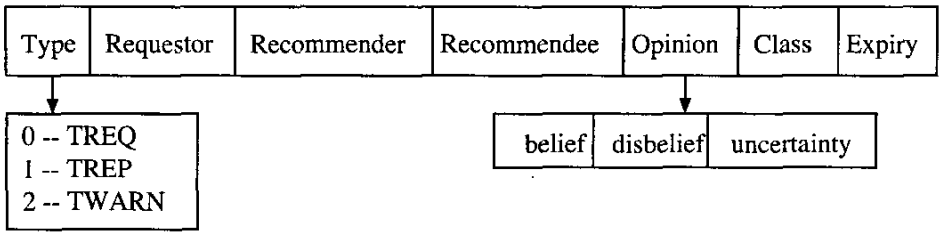


Figure 3. Message Structure of Trust Recommendation Protocol

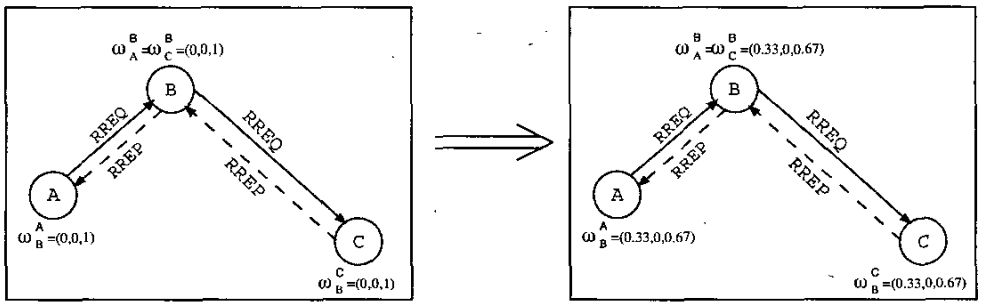


Figure 4. Initialization for TAODV

(1) 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 $\omega_A^B = \omega_C^B = (0, 0, 1)$.

(2) 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 $\omega_A^B = (0, 033\ , 0.67)$. B will not forward the RREQ.

(3) 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.

Scenario II: A TAODV MANET after a period of running time—In this case, a stable MANET has run for a period of time and the trust relationships have been established among almost all the nodes. Consequently, we can give a general description of trusted routing discovery process as follows.

In the beginning of a MANET, because almost all the nodes are uncertain about other nodes' trustworthiness and authenticity, they have to authenticate with each other when performing routing behaviors. With the opinions being updated from time to time, the third component *uncertainty* of opinion will be decreased and the trust relationships among nodes are formed. Nodes will thus employ the combination of different opinions to authenticate one another. The combination method is derived from the subjective logic introduced in Section 2.

We describe the trust authentication algorithm and formulate the general procedure when performing trusted routing discovery in the following, which can be illustrated in Figure 5. In Figure 5, the route path from the source node S to the target node T is totally uncovered. Node $N2$ is the most important intermediate node during the establishment of a route path from S to T. The behaviors of $N2$, then, is described in Algorithm 1 for trusted routing discovery and Algorithm 2 for its authentication function.

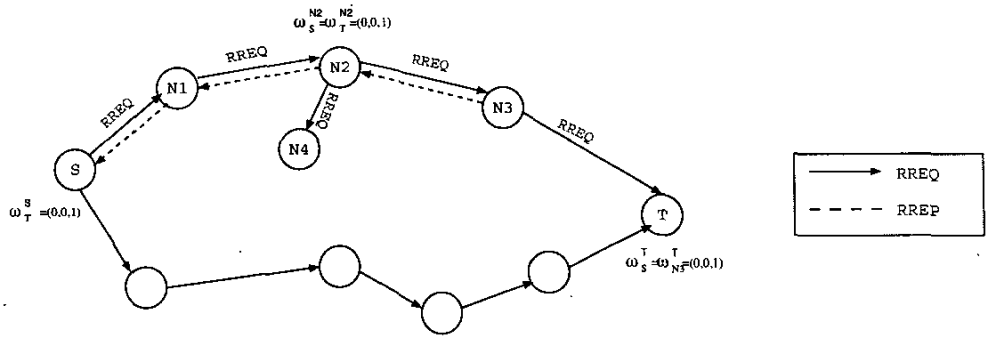


Figure 5. An Example for Trusted Routing Discovery

Algorithm 1 General Procedure of Node $N2$ in Performing Trusted Routing Discovery

Receive an RREQ(S,T) from $N1$

if Authenticate($N2, N1$) == true **then**
  if Authenticate($N2, S$) == true **then**
    if Authenticate($N2, T$) == true **then**
      Update opinion ω_{N1}^{N2}, ω_{S}^{N2}, ω_{T}^{N2}
      Update route table of $N2$
      Re-broadcast RREQ
    end if
  end if
end if

if Every authentication fails **then**
  Update opinion
  Do not forward RREQ
end if

Algorithm 2 Authenticate Function of Node $N2$ to Node $N1$

Exchange opinions about $N1$ with all the neighbors of $N2$ using the trust recommendation protocol (Section 5)

Combine these opinions together using trust combination algorithms (Section 2)

/*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**
  Distrust $N1$ for an expiry time
else if belief> 0.5 **then**
  Trust $N1$ and re-broadcast RREQ/RREP
else
  /*Do not have much confidence about $N1$'s trustworthiness.*/
  Request and verify $N1$'s certificate, by default
end if

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

By introducing the idea of the trust model into our design, we are able to establish a more flexible and less overhead secure routing protocol for MANETs.

From performance point of view, our trusted routing protocol introduces less computation overheads than other security solutions for MANETs. This design does not need to perform cryptographic computations in every packet, which will cause huge time and performance consumption. After the trust relationships is established, the subsequent routing operations can be performed securely according to trust information instead of certificates all the time. Therefore, the TAODV routing protocol improves the performance of security solutions. Unlike some previous security schemes [3] [4], whose basis of routing operations is "blind un-trust", TAODV do not decrease the efficiency of routing discovery and maintenance.

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

From flexibility point of view, our security scheme 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. 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. In summery, 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.

8. Acknowledgements

The work described in this paper was fully supported by a grant from the Research Grants Council of the Hong Kong Special Administrative Region, China (Project No. CUHK4182/03E).

References

[1] 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.

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

[3] 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.

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

[5] 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.

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

[7] 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.

[8] L. Zhou and Z. J. Haas, "Securing ad hoc networks," *Journal of IEEE Networks*, vol. 13, no. 6, pp. 24–30, 1999.

[9] 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.

[10] 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.

[11] 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.

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

[13] A. Josang, "A logic for uncertain probabilities," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 9, no. 3, pp. 279–311, 2001.

[14] ——, "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.

[15] ——, "Prospectives for modelling trust in information security," in *Proceedings of Australasian Conference on Information Security and Privacy*, 1997, pp. 2–13, http://citeseer.nj.nec.com/josang97prospectives.html.

[16] 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.

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

[18] R. Yahalom, B. Klein, and T. Beth, "Trust relationships in secure systems - a distributed authentication perspec-

tive," in *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy (RSP '93)*, 1993, pp. 150–164.

[19] A. Abdul-Rahman and S. Halles, "A distributed trust model," in *Proceedings of New Security Paradigms Workshop '97*, 1997, pp. 48–60.

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

[21] 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.

[22] 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: Springer-Verlag, April 2002, http://citeseer.nj.nec.com/eschenauer02trust.html.

[23] 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.

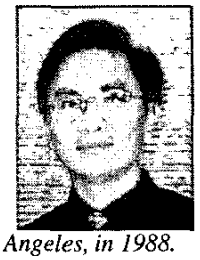
[24] D. B. Johnson and D. A. Maltz, "Dynamic source routing protocol in ad hoc wireless networks," in *Mobile Computing*, T. Imielinski and H. Korth, Eds. Boston, USA: Kluwer Academic Publishers, 1996, ch. 5, pp. 153–181.

[25] 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)*. London, UK: ACM Press, 1994, pp. 234–244, http://doi.acm.org/10.1145/190314.190336.

[26] 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)*. Boston, Massachusetts, USA: ACM Press, 2000, pp. 275–283, http://doi.acm.org/10.1145/345910.345958.

[27] 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))*, 2000, pp. 255–265, http://citeseer.nj.nec.com/marti00mitigating.html.

Xiaoqi Li *received the M.S. degree in computer science and technology from Harbin Institute of Technology, Harbin, China, in 2000. Now she is a Ph.D. candidate in the Department of Computer Science and Engineering at the Chinese University of Hong Kong. Her research interests include wireless security issues, especially the security solutions for mobile ad hoc networks, and protocol design.*

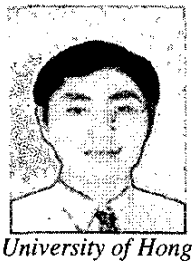


Michael R. Lyu *received the B.S. degree in electrical engineering from National Taiwan University, Taipei, Taiwan, China, in 1981, the M.S. degree in computer engineering from University of California, Santa Barbara, in 1985, and the Ph.D. degree in computer science from University of California, Los Angeles, in 1988.*

He is currently a Professor in the Department of Computer Science and Engineering, The Chinese University of Hong Kong, Shatin, Hong Kong. He was with the Jet Propulsion Laboratory as a Technical Staff Member from 1988 to 1990. From 1990 to 1992, he was with the Department of Electrical and Computer Engineering, The University of Iowa, Iowa City, as an Assistant Professor. From 1992 to 1995, he was a Member of the Technical Staff in the applied research area of Bell Communications Research (Bellcore), Morristown, New Jersey. From 1995 to 1997, he was a Research Member of the Technical Staff at Bell Laboratories, Murray Hill, New Jersey. His research interests include software reliability engineering, distributed systems, fault-tolerant computing, wireless communication networks, Web technologies, digital libraries, and E-commerce systems. He has published over 150 refereed journal and conference papers in these areas. He received Best Paper Awards in ISSRE'98 and ISSRE'2001. He has participated in more than 30 industrial projects, and helped to develop many commercial systems and software tools. He was the editor of two book volumes: Software Fault Tolerance (New York: Wiley, 1995) and The Handbook of Software Reliability Engineering (Piscataway, NJ: IEEE and New York: McGraw-Hill, 1996).

Dr. Lyu initiated the First International Symposium on Software Reliability Engineering (ISSRE) in 1990. He was the program chair for ISSRE'96, and has served in program committees for many conferences, including ISSRE, SRDS, HASE, ICECCS, ISIT, FTCS, DSN, ICDSN, EUROMICRO, APSEC, PRDC, PSAM, ICCCN, ISESE, and WWW. He was the General Chair for ISSRE2001, and the WWW10 Program Co-Chair. He has been frequently invited as a keynote or tutorial speaker to conferences and workshops in U.S., Europe, and Asia. He has been an Associate Editor of IEEE Transactions

on Reliability, IEEE Transactions on Knowledge and Data Engineering, and Journal of Information Science and Engineering. Dr. Lyu is a fellow of IEEE.



***Jiangchuan Liu** received the B.Eng degree (cum laude) from Tsinghua University, Beijing, China, in 1999, and the Ph.D. degree from The Hong Kong University of Science and Technology in 2003, both in computer science. He joined the Department of Computer Science and Engineering of The Chinese University of Hong Kong as Assistant Professor in 2003. He is also a Microsoft Research Fellow, and conducted research at Microsoft Research, Asia, in the summers of 2000, 2001 and 2002. He won first-class honors in several national or regional programming contests, and holds one European patent (granted) and two US patents (pending).*

His current research interests include multicast protocols, streaming media, wireless ad hoc networks, and service overlay networks. He is a TPC member and Information System Co-Chair of IEEE INFOCOM'04, and a guest editor of ACM/Kluwer Journal of Mobile Networks and Applications (MONET), special issue on wireless sensor networks.