Trust Evaluation Based Security Solution in Ad Hoc Networks

Zheng Yan[1], Peng Zhang[2], Teemupekka Virtanen[3]

[1] Nokia Research Center, Nokia Group, Helsinki, Finland
[2] Nokia Venture Organization, Nokia Group, Helsinki, Finland
[3] Helsinki University of Technology, Finland
{zheng.z.yan, peng.p.zhang}@nokia.com,
teemupekka.virtanen@hut.fi

Abstract. Ad hoc networks are new paradigm of networks offering unrestricted mobility without any underlying infrastructure. The ad hoc networks have salient characteristics that are totally different from conventional networks. These cause extra challenges on security. In an ad hoc network, each node should not trust any peer. However, traditional cryptographic solution is useless against threats from internal compromised nodes. Thus, new mechanisms are needed to provide effective security solution for the ad hoc networks. In this paper, a trust evaluation based security solution is proposed to provide effective security decision on data protection, secure routing and other network activities. Logical and computational trust analysis and evaluation are deployed among network nodes. Each node's evaluation of trust on other nodes should be based on serious study and inference from such trust factors as experience statistics, data value, intrusion detection result, and references of other nodes, as well as node owner's preference and policy. In order to prove the applicability of the proposed solution, authors further present a routing protocol and analyze its security over several active attacks.

KEYWORDS: trust, security, ad hoc networks

1 Introduction

Ad hoc networks are new paradigm of networks offering unrestricted mobility without any underlying infrastructure. An ad hoc network is a collection of autonomous nodes or terminals that communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner. Each node functions as both a host and a router. More critically, the network topology is in general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes. There are two major types of wireless ad hoc networks: Mobile Ad Hoc Networks (MANETs) and Smart Sensor Networks (SSNs) [1]. In this paper, our discussion will

mainly focus on the MANETs. Significant applications of MANETs include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks that cannot rely on centralized and organized connectivity.

Operation in an ad hoc network introduces new security problems. The ad hoc networks are generally more prone to physical security threats. The possibility of eavesdropping, spoofing, denial-of-service, and impersonation attacks increases [1]. Similar to fixed networks, security of the ad hoc networks is considered from the attributes such as availability, confidentiality, integrity, authentication, non-repudiation, access control and usage control [2, 3]. But security approaches used for the fixed networks are not feasible due to the salient characteristics of the ad hoc networks. New threats, such as attacks raised from internal malicious nodes, are hard to defend [4]. New security mechanisms are needed to adapt the special characteristics of the ad hoc networks.

Trust is an important aspect in the design and analysis of secure distribution systems [5]. It is also one of the most important concepts guiding decision-making [6]. Trust is a critical part of the process by which relationships develop [7]. It is a before-security issue in the ad hoc networks. By clarifying the trust relationship, it will be much easier to take proper security measures, and make correct decision on any security issues. A trust model specifies, evaluates and sets up trust relationship among entities. Trust modeling is a technical approach to represent trust for digital processing. Recently, trust modeling is paid more and more attention in electronic systems. Current trust academic work covers such aspects as analyzing the problems of current secure systems [8, 9], proposing models for achieving trust in digital systems [10-12] and quantifying or specifying trust in digital systems [13,14].

In this paper, the authors study the security problems in the ad hoc networks and propose a trust evaluation based security solution. The rest of the paper is organized as follows. Section two discusses the security problems in the ad hoc networks. Section three presents the current security schemes in the literature. In section four, a trust evaluation based solution for the ad hoc networks is proposed. In the next section, the solution is illustrated by a routing protocol and proved by analyzing its security against several active attacks. In section six, the authors further discuss the solution and present its characteristics. Finally, the conclusions and directions of future work are given in the last section.

2 Security Problems in Ad Hoc Networks

The salient characteristics of the ad hoc networks pose challenges to security [2-4].

First of all, the use of wireless link renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active interfering. Unlike fixed hardwired networks with physical defense at firewalls and gateways, attacks on an ad hoc network can come from all directions and target at any node. Damage includes leaking secret information, interfering message and impersonating nodes, thus

violating the basic security requirements. All these mean that every node must be prepared for encounter with an adversary directly or indirectly.

Secondly, autonomous nodes in an ad hoc network have inadequate physical protection, and therefore more easily to be captured, compromised, and hijacked. Malicious attacks could be launched from both outside and inside the network. Because it is difficult to track down a particular mobile node in a large scale of ad hoc network, attacks from a compromised node are more dangerous and much harder to detect. All these indicate that any node must be prepared to operate in a mode that should not immediately trust on any peer.

Thirdly, any security solution with static configuration would not be sufficient because of the dynamic topology of the networks. In order to achieve high availability, distributed architecture without central entities should be applied. This is because introducing any central entity into security solution may cause fatal attack on the entire network once the centralized entity is compromised. Generally, decision making in the ad hoc networks is decentralized and many ad hoc network algorithms rely on the cooperation of all nodes or partial nodes. But new type of attacks can be designed to break the cooperative algorithm. Malicious nodes could simply block or modify the data traffic traversing them by refusing the cooperation or hacking the cooperation. As can be seen from the above, no matter what security measures are deployed, there is always some vulnerability that can be exploited to break in.

It seems difficult to provide a general security solution for the ad hoc networks. Traditional cryptographic solution is not adapted for the new paradigm of the networks. As can be seen from the above analysis, what is lacked in the ad hoc networks is trust since each node must not trust any other node immediately. If the trust relationship among the network nodes is available for every node, it will be much easier to select proper security measure to establish the required protection. It will be wiser to avoid the un-trusted nodes as routers. Moreover, it will be more sensible to reject or ignore hostile service requests. Therefore, the trust evaluation becomes a before-security issue in the ad hoc networks. The security solution should be dynamic based on the changed trust relationship.

3 Related Work

Current security study for the ad hoc networks is scattered on special topics such as intrusion detection, secure routing, and key management.

3.1 Intrusion detection

The ad hoc networks have inherent vulnerabilities that are not easily preventable. Intrusion prevention measures, such as encryption and authentication, are required to protect network operation. But these measures cannot defend compromised nodes, which carry their private keys. Intrusion detection presents a second wall of defense.

It is a necessity in the ad hoc networks to find compromised nodes promptly and take corresponding actions to against. A distributed and cooperative architecture for better intrusion detection was proposed in [3]. Based on the proposed architecture, a statistical anomaly detection approach is used. The detection is done locally in each node and possibly through cooperation with all nodes in the network. But how to define the anomaly models based on which trace data is still a main challenge.

3.2 Secure routing

In the ad hoc networks, routing protocol should be robust against topology update and any kinds of attacks. Unlike fixed networks, routing information in an ad hoc network could become a target for adversaries to bring down the network. There are two types of threats. The first one comes from external attackers. The attacks include injecting erroneous routing information, replaying old routing information, and distorting routing information. With these ways, the attackers can successfully partition a network or introduce excessive traffic load into the network, thus cause retransmission and ineffective routing. Using cryptographic schemes, such as encryption and digital signature can defend against the external attacks. The second threat comes from compromised nodes, which might send malicious routing information to other nodes. Typical attacks fallen into this category are black hole attacks, routing table overflow attacks, impersonation and information disclosure, etc. [4]. The internal attacks from malicious nodes are more severe because it is very difficult to detect because the compromised nodes can also generate valid signature. Existing routing protocols cope well with the dynamic topology, but usually offer little or no security measures [2].

In [18], a set of design techniques for intrusion resistant ad hoc routing algorithm (TIARA) was presented mainly to against denial-of-service attacks. Secure aware ad hoc routing (SAR) in [15] uses security properties (e.g. time stamp, sequence number, authentication password or certificate, integrity, confidentiality, and non-repudiation) as a negotiable metric to discover secure routes in an ad hoc network. The SAR can be implemented based on any on-demand ad hoc routing protocol with suitable modification. But it only considers the effect of security properties on the trust. In [4], a secure routing solution is proposed for the black hole problem. But unfortunately, this solution does not solve the problem caused by cooperation of multiple malicious nodes.

3.3 Key management

Traditional cryptographic mechanisms, such as digital signature and public key encryption, still play vital roles for the security of the ad hoc networks. All these mechanisms require a key management service to keep track of key and node binding and assist the establishment of mutual authentication between communication nodes. Traditionally, the key management service is based on a trusted entity called a certificate authority (CA) to issue public key certificate of every node. The trusted CA

is required to be online in many cases to support public key revocation and renewal. But it is dangerous to set up a key management service using a single CA in an ad hoc network. It will be the vulnerable point of the network. If the CA is compromised, the security of the entire network is crashed. In [2] and [16], a threshold cryptography is used to provide robust and ubiquitous security support for the ad hoc networks. The CA functions are distributed through a threshold secret sharing mechanism. This approach is very complicated to implement. It is also hard to survive from multiple hijacked nodes that have secret shares.

The security for the ad hoc networks is still in its infancy. Existing solutions cannot solve this issue well. What is missed is an effective mechanism that can provide reasonable inference based on available knowledge, such as intrusion detection result, past experience, communication data value, and preferences, to evaluate trust relationship among network nodes. With the evaluation result, it is possible to make correct decision or close-correct decision on security protection. New mechanisms are expected to adapt the special characteristics of the new network paradigm.

4 Trust Evaluation Based Security Solution

In this section, the authors propose a trust evaluation based security solution for the ad hoc networks. It introduces a fair and rational security mechanism into the ad hoc networks by simulating human being's decision-making procedure. The perfect security may not be reached, but the average security level should be satisfied based on accumulated knowledge and experience, as well as trust relationship established and adjusted. The decision-making on data protection approach, secure route selection, and any other activities related to security should be based on trust analysis and evaluation.

4.1 Trust modeling

Trust modeling is a technical approach to represent trust for digital processing. Herein, two trust models are proposed based on two ad hoc system models. One is an independent model that represents independent ad hoc networks without any connection to the fixed networks, as shown in Figure 1. The other is a cross model that represents ad hoc networks with few connections to the fixed networks, as shown in Figure 2. In both models, the basic unit that represents an ad hoc node is a Personal Trusted Bubble (PTB). In the bubble, the owner of the ad hoc device has illogically full trust on the device, which is responsible for the ad hoc communication and organization. Among bubbles and between the bubbles and the fixed networks, logical and rational trust relationship should be evaluated computationally. The above trust evaluation is conducted digitally ahead of any communication and the evaluation result should be considered for better security decision.

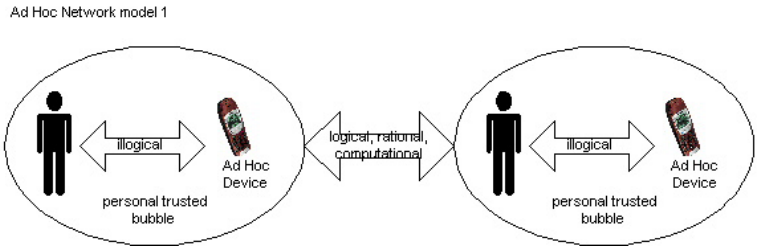

Fig. 1. Independent model (without connection to fixed networks)

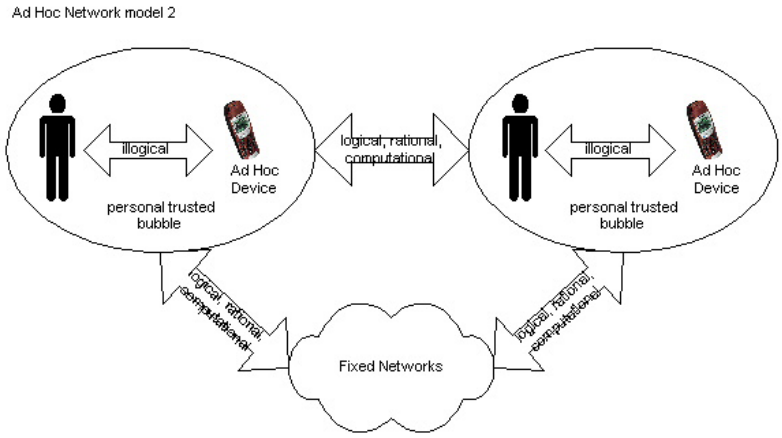

Fig. 2. Cross model (with few connections to fixed networks)

4.2 Trust evaluation mechanism

Based on the study of the trust definition in [17], it is understood that trust is a concept hard to define because it is itself a vague term. The trust defined herein is the confidence of an entity (PTB) on another entity (PTB) based on the expectation that the other entity will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other entity. The level of trust considered sufficient may be different for different individuals (ad hoc device owners in PTB – PTB owners). It is also dynamic because it is affected by many changeable factors.

In the modeled ad hoc networks, the trust evaluation mechanism is introduced into each PTB. The trust relationship between the host bubble and other bubbles is evaluated digitally according to the knowledge accumulated and subjective factors of the bubble owner. In each bubble, there is a trust matrix which stores the knowledge

used for trust evaluation on every other bubble, as show in Figure 3. The factors that may affect the trust are as follows. Note B(i) stands for a PTB (i.e. a node in the ad hoc networks described below).

B(i)	experience statistics	data value	reference	personal preference	PTB policy	intrusion black list	..... others
B(1)	Ves(i,1)	Vd(i,1)	Vr(i,1)	rx(i, 1, a)	Vp(i,1, a)	1/0	Vo(i,1)
B(2)	Ves(i,2)	Vd(i,2)	Vr(i,2)	rx(i, 2, a)	Vp(i,2, a)	1/0	Vo(i,2)
...							
B(i-1)	Ves(i,i-1)	Vd(i,i-1)	Vr(i,i-1)	rx(i, i-1, a)	Vp(i, i-1, a)	1/0	Vo(i,i-1)
B(i+1)	Ves(i,i+1)	Vd(i,i+1)	Vr(i,i+1)	rx(i, i+1, a)	Vp(i, i+1,a)	1/0	Vo(i,i+1)
...							
B(n)	Ves(i,n)	Vd(i,n)	Vr(i,n)	rx(i, n, a)	Vp(i, n, a)	1/0	Vo(i,n)

Fig. 3. Trust evaluation matrix

Experience statistics: This is statistic data of prior experience accumulated during the communications with other nodes. The communication success through some node will increase the trust index of that node. The communication failure through that node will decrease the trust index attached to that node. Just like human being's communications, the trust we established on one person is generally based on the proportion of communication success and the level of satisfaction. By digitizing the value of the experience statistics, its value can be expressed as:

$V_{es}(i, j) = F_{ES}$ (proportion of successful communication between B(i) and B(j), level of satisfaction from B(i) to B(j)), where F represents a function.

Data value: This is the value of communication data. The higher value of data, the higher trust needed from other PTBs to transfer. The data value sent from B(i) to B(j) can be expressed as:

$V_d(i, j) = F_D$ (importance of data transferred between B(i) and B(j), security level of the system and B(i))

Intrusion black list: The black list of malicious nodes based on intrusion detection of the host PTB. The value of intrusion black list can be expressed as:

$V_{ibl}(i, j) = 1/0$. 1: B(j) is good node treated by B(i); 0: B(j) is malicious node treated by B(i).

Reference: Some reference, such as other bubbles' recommendation, reputation of the evaluated node, and other PTBs intrusion detection report, may also impact the

final evaluation result, especially when other information is lacked at the beginning of the network running. The value of reference is expressed as:

$V_r(i, j) = F_R$ (other PTBs' recommendation on B(j), reputation of B(j), other PTBs' intrusion detection report on B(j), ……)

Personal preference: The bubble owner's personal preference also affects the decision of trust as a subjective factor. The rate of the trust factor is one example.

$r_x(i, j, a) = F_r$(preferred rate of B(i) on x factor when evaluating trust on B(j) on action a), where x can be *es*, *d*, *r*, etc.
Actually, $r_x(i, j, a)$ is a set of values for different network actions, $r_x(i, j, a) = \{ r_x(i, j, a_k) \mid k = 1,\ldots,n) \}$.

PTB policy: Like the personal preference, the PTB's policy is also a subjective factor that affects the trust evaluation result. It is related to the whole network's security requirements and policy. It also affects the personal preferences. Most importantly, the trust threshold is also decided by the PTB's policy. In addition, the policy can also be tailored for different PTBs. The value of B(i)'s policy on some special action *a* for B(j) can be described as:

$V_p(i, j, a) = F_P$ (network's security policy, B(i)'s security policy on B(j), basic security requirements, ...)
The $V_p(i, j, a)$ is in practice a set of values for different network actions, $V_p(i, j, a) = \{ V_p(i, j, a_k) \mid k = 1,\ldots,n)\}$.

Other factors (e.g., frequency of routing request from a node, energy left, etc) can also be considered in the trust evaluation on particular action if needed. They can be involved into the evaluation based on the preferred evaluation algorithms.
$V_o(i, j) = F_O$ (frequency of routing request message from B(j), energy left on B(i), ...)

Herein, the authors suggest a linear function that can work for the simple trust evaluation. $TE_a(i, j)$ stands for trust evaluation result conducted by B(i) on B(j) for particular action *a*. It is calculated by considering the objective factors tailored by the subjective factors.

$$TE_a(i, j) = [r_{es}(i, j, a)* V_{es}(i, j) + r_d(i, j, a)* V_d(i, j) + r_r(i, j, a)* V_r(i, j) + r_o(i, j, a)* V_o(i, j)] * V_{ibl}(i, j)$$

In the above function, $r_x(i, j, a)$ (x = es, d, r, or o) is a factor rate that is decided by the personal preference. The total sum of $r_x(i, j, a)$ is 1 and the value of $r_x(i, j, a)$ may be different for different actions. The experience statistics, data value, reference and other factors can be digitized and applied a digital value. In addition, it is noted that the value of intrusion black list, $V_{ibl}(i, j)$, is either 1 or 0. Therefore, the result of the above function is a value. If the value exceeds the trust threshold $V_p(i, j, a)$ defined by the PTB policy on the particular action, the host PTB (B(i)) can trust the evaluated PTB (B(j)) on that action. If the value is below the trust threshold, the host PTB (B(i)) can avoid using the evaluated PTB (B(j)) or apply corresponding protection to the particular action. Furthermore, the trust evaluation is often conducted on several PTBs. It is easy to compare the digital results and select the most trusted PTB for

intended purpose. Other trust evaluation algorithms (such as those in [19-21]) could also be applied, but they may not be quite adaptive to the ad hoc networks.

5 Secure Routing Based on Trust Evaluation

In this part, a *source-initiated on-demand driven* routing is illustrated as an example to apply the above trust evaluation based security solution into secure ad hoc routing. Here, it is assumed that the ad hoc nodes can authenticate with each other correctly. In order to follow traditional routing description, node herein instead of PTB is used for easy understanding. The routing algorithm is described as follows.

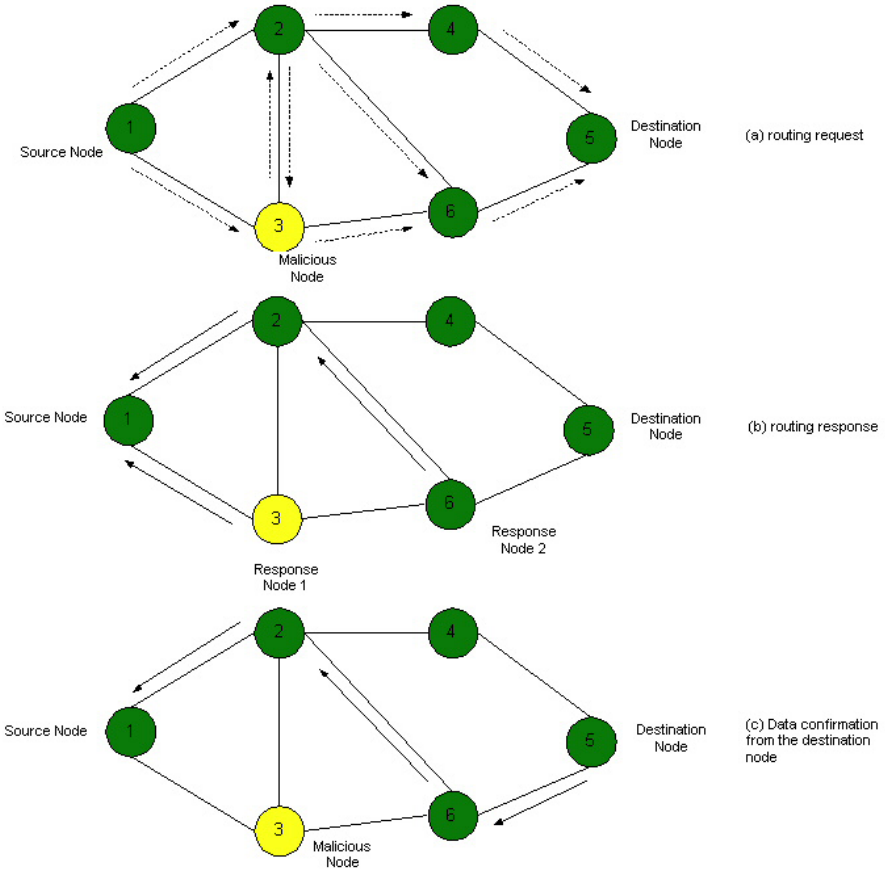

Fig. 4. Secure routing with trust evaluation

1. Source node broadcasts routing request message to its neighbors in order to find a route to destination node.

2. The neighbors of the source node forward the request to their neighbors if the trust evaluation on the source node pass its predefined threshold, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is reached. And that node would like to accept the data transfer based on its trust evaluation. (Figure 4 (a))

3. If some nodes respond that they have fresh enough route to the destination node and would like to reserve some time slot for serving data transfer, the source node checks the trust evaluation matrix and conducts the trust evaluation on the responded nodes. Based on the evaluation result and hops of the routes, the source node selects one preferred route, which it believes the best. (Figure 4 (b))

4. The source node sends (test) data packages to the destination using the selected route and set preferred time slot waiting for the destination node's confirmation and indicates that which package is required to respond confirmation of receival.

5. After receiving the data packages, the destination node applies the same method above to reply the confirmation message if the source node requests it. It is not mandatory to use the same route as the source for better security consideration. (Figure 4 (c))

6. If within the time slot, the destination's confirmation arrives and can be verified as valid, the source node will continue sending data packages via the underlying route. If the destination's confirmation cannot receive within the preferred time slot, the source node will update its trust evaluation matrix data on the routing nodes by reducing the trust value of experience statistics. If the source node makes sure the response node of underlying route is malicious, it will put the node into the intrusion black list, set that value to 0. The source node also propagates the malicious node over the networks. This information is used for updating the reference of other nodes' trust evaluation matrix and the update should also follow the trust evaluation on the source node. Then processing either jumps to step 1 for higher security or goes to step 7 for better performance.

7. The source node selects the second best route. Then go to step 4.

The proposed protocol can be implemented based on any on-demand ad hoc routing protocol with suitable modification and by adding knowledge accumulation and trust evaluation mechanism. Next, we further evaluate the security of our proposed routing protocol by analyzing it over several active ad hoc routing attacks described in [4].

Black hole attacks: In this attack, a malicious node uses the routing protocol to advertise itself as the shortest path to other nodes. The proposed routing protocol can defend this attack because it randomly requires the destination node's confirmation of the data package. If the source cannot receive the confirmation within the indicated time slot, it will change the route. In addition, the confirmation message may not be transferred via the same route as the source node selected. The route of the confirmation message is selected based on the destination's trust evaluation matrix. In addition, the confirmation response is requested randomly by the source node. Therefore, it will greatly reduce the risk that the confirmation message is intentionally

transferred by the malicious node to the source node. What is more, if the malicious node is found by any node in the network, this attack can be avoided in our protocol based on the trust evaluation mechanism.

Denial of service: The DoS attack happens when the network bandwidth is hijacked by a malicious node. Any intrusion detection mechanism can be deployed and its result will contribute to the trust evaluation matrix, therefore affect any security-related decision. For instance, a malicious node might generate frequent route requests to make the network resources unavailable to other nodes. The proposed protocol fights against this attack in the following way. In step 2, the neighbor node processes the routing request according to the trust evaluation, in which the frequency of routing request message from a node is considered as one of main factors. If the frequency of request exceeds the threshold defined in the PTB's policy, the neighbor node will ignore the request. And at the same time, the neighbor node may broadcast the possibility of intrusion in the network. Any intrusion report broadcast in the network is recorded by every node and used for updating the value of reference in the trust evaluation matrix.

Routing table overflow attacks and energy consummation: In the first attack, the attacker attempts to create routes to nonexistent nodes. The goal is to have enough routes so that creation of new routes is prevented or the implementation of routing protocol is overwhelmed. In the second attack, an attacker can attempt to consume batteries by requesting routes or forwarding unnecessary packets to a node. In the proposed protocol, every node has right to ignore or reject route serving or data receiving according to the trust and ability evaluation. And the service time for other nodes can be set according to the evaluation result. In this way, it can be effectively against these kinds of attacks.

6 Further discussion

The security for the ad hoc networks is still in its infancy. Since the ad hoc networks are dynamic by nature, they require a dynamic security solution that fits this fundamental characteristic.

The proposed solution tries to simulate human being's social contact procedure on decision-making and introduces it into the ad hoc networks. The perfect security solution is hard to reach. But the average security level (for a node) can be achieved as expectation based on accumulated knowledge and as well as the trust relationship built and adjusted. With this way, it could greatly reduce security threats. As shown in Figure 5 (a), at the beginning, the security level reached may be quite low because the nodes (potentially malicious) do not have much knowledge about other nodes. With time elapsing, the nodes know each other more and more. So the trust evaluation on particular actions is more and more close to correctness. This causes the security level reaching its expectation. Figure 5 (b) shows another case where every node is a good node and full of capability at the beginning. So the security achieved at the start point is high. With the network running, some nodes are compromised. Some lack energy. Those cause security level to decrease. On the other hand, the trust evaluation is more

and more correct. It directs any decision on security and pushes the security level reaching the expectation.

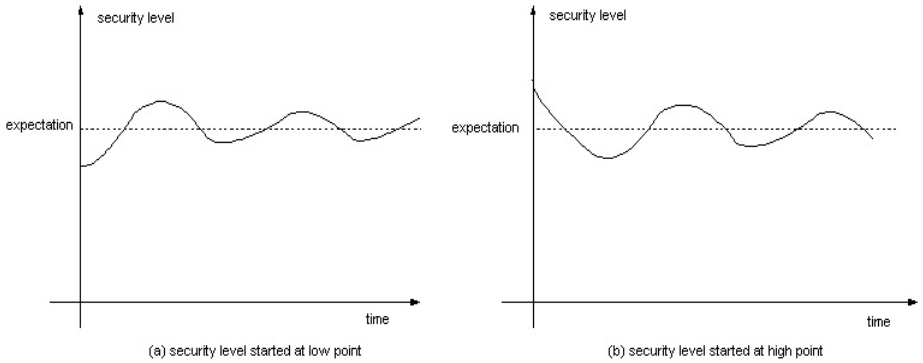

Fig. 5. Gradual security achievement

But the above trust evaluation result may not keep correct longer because of the dynamic characteristic of the network and its vulnerabilities. Further understanding is needed among the nodes. The trust evaluation will be close to correctness gradually since knowledge and experience accumulated by every node should not be updated frequently and totally. This is because the possibility of the whole network crash is low.

Even though there are some problems left, this method will help in avoiding further loss. The proposed mechanism is also flexible to resist new attacks by introducing new factors into the trust evaluation. Due to the dynamic characteristics of the networks, it is suggested that the trust evaluation should be conducted at real time if the security requirement is high. The authors call this solution as gradual-security approach.

7 Conclusions and future work

The new paradigm of the ad hoc networks presents new challenges on security due to its salient characteristics that are totally different from the conventional wired and wireless networks. In this paper, the authors studied the security issues in the ad hoc networks and analyzed the problems. The existing solutions cannot solve the security issues for the ad hoc networks well.

Based on the study, a trust evaluation based security solution was proposed by introducing human being's social contact procedure into any security-related decision-making. The authors believe that data protection approach, secure route selection, and any other decision related to security should be based on trust analysis and evaluation among network nodes. Based on this mechanism, the authors further applied the

mechanism to a *source-initiated on-demand driven* routing protocol and analyze its security over several active attacks. The analysis showed that the proposed protocol against those attacks effectively. In addition, we further discussed the solution as a gradual-security solution, which can achieve average security level as expectation based on knowledge and experience accumulation and inference. It is hard to achieve perfect security, but it is possible to greatly reduce the threats.

Immediate future work includes study of efficient and effective trust evaluation algorithm, simulation and proof of the proposed routing protocol. The authors are also working on how to establish basic trust identity to enforce the trust analysis and evaluation are conducted on the correct target nodes.

References

[1] S. Corson, J. Macker. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. IETF RFC2501, 1999.

[2] L. Zhou, Z. J. Haas. Securing Ad Hoc Networks. IEEE Network, 13(6): 24-30, Nov/Dec 1999.

[3] Yongguang Zhang, Wenke Lee. Intrusion Detection in Wireless Ad-Hoc Networks. Proceedings of MobiCom 2000, Sixth Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6-11 Aug. 2000.

[4] HongMei Deng, Wei Li, Dharma P. Agrawal. Routing Security in Wireless Ad Hoc Networks. IEEE Communications Magazine, October 2002, p70-75.

[5] Diamadi, Z. Fischer, M.J. A simple game for the study of trust in distributed systems. International Software Engineering Symposium 2001 (ISES'01), Wuhan University Journal of Natural Sciences Conference. March 2001.

[6] Shillo, M.; Funk, P.; Rovatsos, M. Using trust for detecting deceitful agents in artificial societies. Applied Artificial Intelligence, vol.14, no.8, p.825-48 Sept. 2000.

[7] Warne, D., Holland, C.P. Exploring trust in flexible working using a new model. BT Technology Journal, vol.17, no.1, p.111-19. Jan 1999.

[8] Gerck Ed. Overview of Certification System: X.509, PKIX, CA, PGP & SKIP. In http://www.thebell.net/papers/certover.pdf

[9] Perlman, R. An overview of PKI trust models. IEEE Network, vol.13, no.6 p.38-43.

[10] Yao-Hua Tan. Thoen, W. Toward a generic model of trust for electronic commerce. International Journal of Electronic Commerce vol.5, no.2, p.61-74.

[11] Egger Florian N. Towards a Model of Trust for E-Commerce System Design. In Proc. Of the CHI2000 Workshop: Designing Interactive Systems for 1-to-1 E-commerce.

[12] Abdul-Rahman Alfarez, Halles Stephen. A Distributed Trust Model. In Proc. Of New Security Paradigms Workshop, ACM, New York, NY, USA, 1998.

[13] Daniel W. Manchala, Xerox Research and Technology. E-Commerce Trust Metrics and Models. IEEE Internet Computing, vol.4, no.2 p.36-44, 2000.

[14] Mui Lik, Mohtashemi Mojdeh, Halberstadt Ari. A Computational Model of Trust and Reputation. In Proc. Of the 35th Annual Hawaii International Conference on System sciences, 7-10 Jan. 2002, Big Island, HI, USA

[15] Seung Yi, Prasad Naldurg, Robin Kravet. Security-aware ad hoc routing for wireless networks. http://www.cs.uiuc.edu/Dienst/Repository/2.0/Body/ncstrl.uiuc_cs/UIUCDCS-R-2001-2241/pdf

[16]Jiejun-K, Petros-Z, Haiyun-Luo, Songwu-Lu, Lixia-Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks. Proceedings Ninth International Conference on Network Protocols. ICNP 2001, Riverside, CA, USA, 11-14 Nov. 2001

[17]McKnight, D. Harrison, Chervany Norman L. What is Trust? A Conceptual Analysis and An Interdisciplinary Model. In Proceedings of the 2000 Americas Conference on Information Systems (AMCI2000). AIS, Long Beach, CA, August 2000..

[18]Ramanujan-R, Ahamad-A, Bonney-J, Hagelstrom-R, Thurber-K. Techniques for intrusion-resistant ad hoc routing algorithms (TIARA). Proceedings of IEEE Military Communications Conference (MILCOM'00), vol.2, Los Angeles, CA, USA, 22-25 Oct. 2000.

[19]A.Jøsang. *An Algebra for Assessing Trust in Certification Chains*. In J.Kochmar, editor, Proceedings of the Network and Distributed Systems Security (NDSS'99) Symposium, The Internet Society, 1999.

[20]Daniel W. Manchala: Xerox Research and Technology. E-Commerce Trust Metrics and Models. IEEE Internet Computing, vol.4, no.2 p.36-44 (2000).

[21]Mui Lik, Mohtashemi Mojdeh, Halberstadt Ari: A Computational Model of Trust and Reputation. In Proc. Of the 35th Annual Hawaii International Conference on System sciences, 7-10 (Jan. 2002), Big Island, HI, USA.