A Cooperative Secure Routing Protocol based on Reputation System for Ad Hoc Networks

Yihui Zhang
Key Laboratory of Network Security and Cryptology/Fujian Normal University, Fuzhou, China
Email: zyh_1983@126.com

Li Xu and Xiaoding Wang
Key Laboratory of Network Security and Cryptology/Fujian Normal University, Fuzhou, China
Email: xuli@fjnu.edu.cn; Wangdin1982@yahoo.com.cn

***Abstract*—In wireless ad hoc networks, all its nodes behave as routers and take part in its discovery and maintenance of routes to other nodes. Thus, the presence of selfish or malicious nodes could greatly degrade the network performance and might even result in a total communication breakdown. However, the majority of ad hoc networks secure routing protocols assumed that all nodes participating in the network are cooperative to support different network functionalities and did not provide a complete solution against these attacks. In this paper, we propose a cooperative secure routing protocol based on reputation system (CSRAN) for wireless ad hoc networks to defend against these attacks efficiently. It is based on ARAN secure routing protocol and detailed analysis is given to show it proves to be more efficient and more secure than original ARAN secure routing protocol in defending against both malicious and authenticated selfish nodes.**

***Index Terms*—Ad hoc networks, reputation system, secure routing protocol**

I. Introduction

Due to the open wireless medium, the routing protocols of Ad-hoc networks are more vulnerable to various attacks than wired networks. Dynamic topology, cooperative algorithms, lack of centralized monitoring and management point also introduce risks to it. Moreover, since all its nodes behave as routers and take part in its discovery and maintenance of routes to other nodes in the network, the significance of node cooperation makes network survival particularly sensitive to insider node behavior. The presence of selfish or malicious nodes could greatly degrade the network performance and might even result in a total communication breakdown. All of these challenges above make new demands to MANET routing protocols.

Reputation management system [1~4] has been proposed to help to enforce node cooperation in ad hoc networks. Basically, a reputation management system works on evaluating nodes’ quality of behavior based on their cooperation (evaluation), distinguishing between well-behaved and misbehaving nodes (detection), and appropriately reacting to misbehaving nodes (reaction). However, few of these proposed cooperation enforcement schemes are based on any existing MANET secure routing protocols. Most of these proposed schemes were based on routing protocols without any security measures at all.

The purpose of this paper is to design an efficient secure on-demand routing protocol integrates with reputation system in wireless ad hoc networks. Detailed analysis is given to show our scheme can not only ensure the security of the routing protocol against most common known attacks, but also improve network throughput and performance.

II. Related Works

In mobile ad hoc networks, packet forwarding, routing and other network basic functions are performed by all nodes instead of dedicated ones. Thus, network operation can be easily jeopardized if security countermeasures are not embedded into basic network functions. Providing security for routing protocol in mobile ad hoc networks is a challenging task and many researchers have engaged in designing various protocols for it.

In the table Ⅰ, a comparison between some of the most established secure routing protocols with respect to some performance and security parameters is given[15]. The respective meaning of Reac., Proac., Sym. and Asym. in the table is reactive, proactive, symmetric and asymmetric .

In addition, a significant number of reputation management systems [1～4] have been proposed for ad hoc networks. In [1], Watchdog and Pathrater components employed to mitigate routing misbehavior have been proposed. The watchdog complemented with DSR is used for detection of denied packet forwarding and the Pathrater is used for rating every candidate path and choose appropriate route according to routing policy, which enable nodes to avoid malicious nodes included in

Corresponding Author: Dr.Xu Li.

This work is supported by National Natural Science Foundation of China (60502047), Education Bureau of Fujian Province (JA07030), Natural Science Foundation of Fujian Province (2008J0014).

TABLE I.
A COMPARISONS OF ESTABLISHED SECURE ROUTING PROTOCOLS IN AD HOC NETWORKS

PROTOCOL	ARIANE	ARAN	SEAD	SRP	SAODV
ITEM	[10]	[11]	[12]	[13]	[14]
Type	Reac.	Reac.	Proac.	Reac	Reac.
Encryption Algorithm	Sym.	Asym.	Sym.	Sym.	Asym.
Synchronization	Y	N	Y	N	N
Central Trust Authority Required	N	Y	Y	Y	Y
Authentication	Y	Y	Y	Y	Y
Confidentiality	Y	Y	N	N	N
Integrity	Y	Y	N	Y	Y
Non-Repudiation	N	Y	Y	N	N
Anti-Spoofing	Y	Y	Y	N	Y

the routes. However, the nodes do not exchange reputation information with other nodes and only rely on their own watchdog exclusively, thus it is inefficient. In fact, the focus of this strategy is the throughput of the networks. CONFIDANT [2] also uses a reputation system to extend reactive routing protocols by isolating misbehave nodes. It detects malicious nodes by means of observation or reports about several types of misbehaviors and thus allows nodes to route around thus isolate misbehaved nodes from the network. However, the protocol trusts second-hand information unconditionally, which can be vulnerabilities in the presence of liars. Josang and Ismail [3] use a Bayesian approach, which centralizes and discounts the belief in second-hand information according to the reputation of agents, equating the trustworthiness of an agent as a witness with its performance in the base system. However, lying nodes that aim at changing the reputation of another node can still perform normally in the base system.

Thus, there is a trade-off problem between efficiency in using the available information and robustness against false ratings. If the ratings made by others (the second-hand information) are considered, the reputation system can be vulnerable to false accusations or false praise. In other words, it would become less robust. If only one's own experience (the first-hand information) is considered, the system would be inefficient, either. Thus, how to balance robustness and efficiency should be settled first in the reputation system. In [5], the author proposed a robust and efficient reputation system for Ad Hoc networks. It adopts a mechanism that makes use of all the available information to enhance the reputation system efficiency. To make the reputation system robust, it uses the trust ratings and deviation test to deal with false ratings.

[15] has proposed a reputed authenticated routing for ad hoc networks. It is also based on ARAN, however it adopts a simple reputation system that only uses the first-hand reputation in order to avoid false rating from other nodes, thus it is inefficient. As a result of these comparisons, we ended up choosing to work with ARAN [11] as the selected secure routing protocol incorporated the reputation system in [5].

III. REPUTATION SYSTEM

In this section, we introduce the reputation system we adopt in the secure routing briefly. We assume communication links are bi-directional. Consider an ad hoc network with nodes $N = \{1,2,\cdots,i,\cdots,n\}$.In our approach, a node i maintains two kinds of ratings about every neighboring node j. In the scheme, node i calculates the reputation value and trust value according to a distribution (called the "prior") which is updated as soon as new observations are made or reported. The distribution Beta (α,β) [6] is used for the prior, since it fits Bernoulli distributions and the conjugate is also a beta distribution. Moreover, the advantage of using the Beta function is that it only needs to update two parameters as soon as observations are made or reported.

For clarity, we introduce some denotations in the following:

$F_{i,j}$: the first-hand reputation rating, which represents a summary opinion made by node i about node j only through its first-hand observation, for example, whether j participates the route protocol correctly. It is defined by two numbers, say, (α_n,β_n), which represents the parameters of the beta distribution assumed by node i in its Bayesian view of node j's behavior as an actor in the base system. Initially, (α_0,β_0) is set to (1, 1).

$R_{i,j}$: The reputation rating, which shows the synthetic opinion maintained by node i about node j's behavior as an actor in the system according to its first-hand observation or second-hand information from other nodes. It is also defined by two numbers, say, (χ_n,η_n) and (χ_0,η_0) is set to (1, 1) initially. It is updated on two cases: (1) when the first-hand reputation rating $F_{i,j}$ is updated; (2) when a reputation rating published by some other node k, $F_{k,j}$, is accepted by i.In the former case, the update procedure is the same as for the first-hand $F_{i,j}$. In the latter case, it uses linear pool model merging [7] to incorporate $F_{k,j}$.

$T_{i,j}$: the trust rating shows node i's opinion about how honest node j is as an actor in the reputation system, for example whether the second-hand information published by node j are likely to be true. It is also defined by two numbers, say (λ_n,ν_n) and (λ_0,ν_0) is set to (1, 1) initially. It uses a similar Bayesian approach as $F_{i,j}$ to update.

$\theta^*_{i,j}$: the direct reputation value which represents a summary opinion made by node i about node j only through first-hand observation. $\theta^*_{i,j} = E(F_{i,j})$. $\theta^*_{i,j} \in [0,1]$.

$\theta_{i,j}$: the synthetic reputation value which represents a summary opinion maintained by node i about node j . $\theta_{i,j} = E(R_{i,j})$. $\theta_{i,j} \in [0,1]$.

$\phi_{i,j}$: the trust value shows node i 's summary opinion about how honest node j is as an actor in the reputation system, $\phi_{i,j} = E(T_{i,j})$. $\phi_{i,j} \in [0,1]$.

To take advantage of second-hand information from other nodes, we need a way to incorporate it into the first-hand information of the node itself. We do this as follows. First, whenever node i makes a first hand observation of node j 's behavior, the first-hand reputation rating $F_{i,j}$ and the synthetic reputation rating $R_{i,j}$ are both updated. Second, from time to time, nodes publish their first-hand reputation rating to other nodes to a subset of the neighboring nodes. It is assumed that node i receives first-hand reputation rating $F_{k,j}$ from k about node j .If k is classified as “trustworthy” by i , or if $F_{k,j}$ is consistent with $R_{i,j}$ (in a sense that is clarified in latter section), then $F_{k,j}$ is accepted by i and is used to slightly modify the $R_{i,j}$ Else, the $R_{i,j}$ is not updated. In all cases, the trust rating $T_{i,k}$ is updated. If $F_{k,j}$ is accepted by i , the trust rating $T_{i,k}$ slightly improves, else it slightly worsens. Note that, only first hand information $F_{i,j}$ is published, neither the reputation $R_{i,j}$ nor the trust ratings $T_{i,j}$ is disseminated.

The standard Bayesian method [3] is used to update $F_{i,j}$, $R_{i,j}$ and $T_{i,j}$ then calculate $\theta^*_{i,j}$, $\theta_{i,j}$ and $\phi_{i,j}$ accordingly . However, it gives the same weight to each observation, regardless of its time of occurrence. We want to give less weight to evidence received in the past to allow for reputation fading. Thus we use a modified Bayesian procedure introducing a discount factor to deal with and update in which mends the Bayesian update approach by introducing a moving weighted average. We take the $F_{i,j}$ and $\theta^*_{i,j}$ for example.

Node i models the behavior of node j as an actor in the base system through first-hand observation as follows. Node i thinks that node j misbehaves with probability $\theta^*_{i,j}$. $\theta^*_{i,j}$ is unknown, and node i calculates it according to beta distribution. Assume i makes one individual observation about j . when a new observation is made, say with s_i observed misbehaviors and (1- s_i) observed correct behaviors. Let s_i =1 if this observation is qualified as misbehavior, and s_i =0 otherwise. Call $s_1, s_{2,\dots,} s_n$ the sequence of observations. Then $F_{i,j}$ updates as equation(1) (2):

$$\alpha_n = u\alpha_{n-1} + s_n \, , 0 \le u \le 1 \qquad (1)$$

$$\beta_n = u\beta_{n-1} + (1 - s_n) \, , 0 \le u \le 1 \qquad (2)$$

The weight u is a discount factor for past experiences, which serves as the fading mechanism. After n first hand observations, we can easily derive from Equation (1) (2) that the value of α_n , β_n is:

$$\alpha_n = s_n + us_{n-1} + u^2 s_{n-2} + \cdots + u^{n-1}s_1 + u^n$$

$$\beta_n = u^n + u^{n-1} + \cdots + u + 1 - u^{n-1}s_1 - u^{n-2}s_2 - \cdots - us_{n-1} - s_n$$

Obviously, $\lim_{n\to\infty}(\alpha_n + \beta_n) = \frac{1}{1-u}$. Assume (temporarily) that $\theta^*_{i,j}$ would be constant, it is easy to calculate that: $\mathrm{E}(s_1) = \mathrm{E}(s_2) = \cdots = \mathrm{E}(s_n) = \theta^*_{i,j}$. We would get $\lim_{n\to\infty}\mathrm{E}(\alpha_n) = \frac{\theta^*_{i,j}}{1-u}$, $\lim_{n\to\infty}\mathrm{E}(\beta_n) = \frac{1-\theta^*_{i,j}}{1-u}$. Thus $\forall \varepsilon > 0$, if ε is small enough. Then $\exists n_1, n_2, n_3 \in \mathrm{N}$,

Case: $n \ge n_1$, $\left|\mathrm{E}(\alpha_n) - \frac{\theta^*_{i,j}}{1-u}\right| < \varepsilon$;

Case: $n \ge n_2$, $\left|\mathrm{E}(\beta_n) - \frac{1-\theta^*_{i,j}}{1-u}\right| < \varepsilon$;

Case: $n \ge n_3$, $\left|(\alpha_n + \beta_n) - \frac{1}{1-u}\right| < \varepsilon$

Let $t = \max\{n_{1,} n_2, n_3\}$ when $n \ge t$, $\mathrm{E}(\alpha_n) \approx \frac{\theta^*_{i,j}}{1-u}$, $\mathrm{E}(\beta_n) \approx \frac{1-\theta^*_{i,j}}{1-u}$, $\alpha_n + \beta_n \approx \frac{1}{1-u}$. Thus $\theta_{i,j} = \mathrm{E}[\frac{(\alpha_n)}{(\alpha_n + \beta_n)}] = \mathrm{E}(Beta(\alpha_n, \beta_n))$.

Using the standard Bayesian approach, after a large m observation, $\mathrm{E}(\alpha_n) \approx m\theta^*_{i,j}$, $\mathrm{E}(\beta_n) \approx m(1-\theta^*_{i,j})$. Thus we should select u so that $E(\alpha_n)$ and $E(\beta_n)$ is also inclined to $m^*\theta^*_{i,j}$ and $m^*(1-\theta^*_{i,j})$. Let $u = 1 - \frac{1}{m^*}$ ($m^* \in \mathrm{N}$) and $m^* = \frac{1}{1-u}$ is an integer, where m^* is the order of magnitude of the number of observations over which we believe it makes sense to assume stationary behavior and m^* >t . Thus $\mathrm{E}(\alpha_n) \approx m^*\theta^*_{i,j}$, $\mathrm{E}(\beta_n) \approx m^*(1-\theta^*_{i,j})$.

In addition, whenever the inactivity time expires, we let $\alpha_n = u\alpha_{n-1}$ and $\beta_n = u\beta_{n-1}$ to decay the values of α, β . This is to allow for redemption even in the absence of observations, either due retaliatory exclusion or simply lack of interaction.

Every node can use the same procedure to update $R_{i,j}$ and $T_{i,j}$ then uses these rating to calculate $\theta_{i,j}$ and $\phi_{i,j}$.

Then it will use these values to classify other nodes periodically, according to two criteria: (1) well-behaved/misbehaving (2) trustworthy/untrustworthy. The classification process works as follows. First, node i updates $R_{i,j}$ and $T_{i,j}$ as explained above. Then Node i classifies the behavior and the trustworthiness of node j of according to the equations (3) and (4):

$$\begin{cases} \text{well-behaved} & \text{if } \theta_{i,j} = E(R_{i,j}) = E(\mathrm{Beta}(\chi_n, \eta_n)) < t_r \\ \text{misbehaving} & \text{if } \theta_{i,j} = E(R_{i,j}) = E(\mathrm{Beta}(\chi_n, \eta_n)) \geq t_r \end{cases} \quad (3)$$

$$\begin{cases} \text{trustworthy} & \text{if } \phi_{i,j} = E(T_{i,j}) = E(\mathrm{Beta}(\lambda_n, \nu_n)) < t_u \\ \text{untrustworthy} & \text{if } \phi_{i,j} = E(T_{i,j}) = E(\mathrm{Beta}(\lambda_n, \nu_n)) \geq t_u \end{cases} \quad (4)$$

Where t_r and t_u are the thresholds that the network can tolerate. They are set according to requirements of the network. These ratings are used to make decisions about other nodes. For example, in a mobile ad-hoc network, decisions are made about whether to forward for another node, which path to choose, whether to avoid another node and delete it from the path cache, and whether to warn others about another node. The misbehaving nodes in our paper comprise malicious nodes and selfish nodes.

Ⅳ. ROUTING PROTOCOL DESIGN

In this section, we present an analysis of the robustness of the Authenticated Routing for Ad Hoc Networks (ARAN) in the presence of the different attacks introduced firstly[15].

a) Unauthorized participation: Since all ARAN packets must be signed, a node can not participate in routing without authorization from the trusted certificate server. This access control therefore rests in the security of the trusted authority, the authorization mechanisms employed by the trusted authority, the strength of the issued certificates, and the revocation mechanism.

b) Spoofed Route Signaling: Route discovery packets contain the certificate of the source node and are signed with the source's private key. Similarly, reply packets include the destination node's certificate and signature, ensuring that only the destination can respond to route discovery. This prevents impersonation attacks where either the source or destination node is spoofed.

c) Fabricated Routing Messages: Since all routing messages must include the sending node's certificate and signature, ARAN ensures non-repudiation and prevents spoofing and unauthorized participation in routing.

d) Alteration of Routing Messages: ARAN specifies that all fields of RDP and RREP packets remain unchanged between source and destination. Since both packet types are signed by the initiating node, any alterations in transit would be detected, and the altered packet would be subsequently discarded. Thus, modification attacks are prevented in ARAN.

e) Denial-of-Service Attacks: Denial-of-service (DoS) attacks can be conducted by nodes with or without valid ARAN certificates. In the certificate-less case, all possible attacks are limited to the attacker's immediate neighbors because unsigned route requests are dropped. However, nodes with valid certificates can conduct effective DoS attacks by sending many unnecessary route requests and they will go undetected as the current existing ARAN protocol can not differentiate between legitimate and malicious RREQs coming from authenticated nodes.

It is clear from the above mentioned security analysis of the ARAN protocol that ARAN is a secure MANET routing protocol providing authentication, message integrity, confidentiality and non-repudiation by using certificates infrastructure. As a consequence, ARAN is capable of defending itself against spoofing, fabrication, modification, DoS and disclosure attacks. Therefore, misbehaving behavior coming from a malicious node will be defended against successfully by ARAN. However, the currently existing ARAN secure routing protocol does not account for attacks that are conducted by authenticated selfish nodes as these nodes trust each other to cooperate in providing network functionalities. This results in that ARAN fails to detect and defend against an authenticated selfish node participating in the mobile ad hoc network. Thus, if an authenticated selfish node does not forward or intentionally drop control or data packets, the current specification of ARAN routing protocol can not detect or defend against such authenticated selfish nodes. This weakness in ARAN specification will result in the disturbance of the ad hoc network and the waste of the network bandwidth.

Since most of the attacks performed by malicious unauthenticated nodes can be detected and defended against by the use of the secure routing ARAN protocol, we only need to discuss those attacks performed by authenticated misbehaving nodes that the ARAN protocol can not defend against. We consider the misbehaving nodes in our paper comprise malicious nodes and selfish nodes. ARAN assumes that authenticated nodes are to cooperate and work together to provide the routing functionalities. In fact, a selfish node in the ad hoc networks can use two possible attacks to save its resources: do not participate in routing (do not relay route requests or do not relay route replies) and do not relay data packets. ARAN fails to detect or defend against these attacks, as they focus only on the detection of malicious nodes attacks rather than the authenticated selfish nodes. Thus, we incorporate the Bayesian-based reputation system [5] in a modified ARAN to detect and defend these attacks.

A. Route Discovery

We denote the source node, nodes en route, and the destination node as S, i (i =1, 2, . . ., n), and D, respectively. If a source node S has packets for the destination node D, S initiates a route discovery packet (RDP) and broadcasts it to its neighbors. Once receiving a RDP, intermediate nodes interested in cooperating to route this control packet broadcast it in a random delay to avoid “broadcast storm” and inserts a record of the source, nonce, destination and previous-hop of this packet in its routing records. This process continues until this RDP reaches D. Then D unicasts a route reply packet (RREP) for each RDP packet that it receives using the reverse-path. Each intermediate node receiving this RREP updates its routing table for the next-hop of the RREP and then unicasts this RREP in the reverse-path using the earlier-stored previous-hop node information. The process repeats until the RREP packet reaches S. Finally, S chooses several records from received RREPs and stores in its routing table for the D.

B. Data Transfer Phase

After the route discovery, the source node S and the other intermediate nodes have several RREPs for the same RDP packet. If a source node S has packets for D, S chooses the next-hop node, says A, which has the highest reputation value from the routing table for data transferring then stores its information in the sent-table as the path for its data transfer. Then, S will start a timer before it should receive a data acknowledgement (DACK) from A for this data packet. Afterwards, A will choose the next-hop node which has the highest reputation value from its routing table and store its information in its sent-table as the path of this data transfer. If the packet has originated from a low-reputed node, the packet is put back at the end of the forwarding queue of the current node and if the packet has originated from a high-reputed node, A sends the data packet to the next hop in the route as soon as possible. In addition, A will start a timer, before which it should receive the DACK from its next-hop node for this data packet. This process continues until the data packet reaches D. Once the packet reaches its destination, the destination node D sends a signed data acknowledgement packet (DACK) to the source S. The DACK traverses the same route as the data packet, but in the reverse direction.

C. Reputation Phase

When an intermediate node i receives a data acknowledgement packet (DACK) from its next-hop j, it retrieves the corresponding record inserted in the data transfer phase and updates the reputation rating $R_{i,j}$ using the reputation schemes. Afterwards, it deletes this data packet entry from its sent-table. The process repeats until the DACK reaches S.

D. Timeout Phase

Once the timer for a given data packet expires at a node i (or S) and i has not received the DACK from its next-hop j, i deemed that j may be a selfish node. It will perform the following operations:

a) i regard j performs a misbehavior and updates $F_{i,j}$ using the reputation scheme;

b) i broadcast a request packet containing $F_{i,j}$ to the each neighbor k of j to ask for $F_{k,j}$;

c) i and each k uses linear pool model merging [6] to update $R_{i,j}$ and $R_{k,j}$ as follows:

Assume node i receives the $F_{k,j} = (\alpha_k, \beta_k)$ from node k. The question is how to detect and avoid false reports. The approach is to employ $T_{i,k}$ and deviation test.

If $\phi_{i,k}$ is such that i considers k trustworthy, $F_{k,j}$ is accepted by node i to modify $R_{i,j} = (\chi_r, \eta_r)$ as follows:

$$\chi_{r+1} = w_{i,kj}\alpha_k + \chi_r \qquad 0 \le w_{i,kj} \le 1 \tag{5}$$

$$\eta_{r+1} = w_{i,kj}\beta_k + \eta_r \qquad 0 \le w_{i,kj} \le 1 \tag{6}$$

Where $w_{i,kj}$ is a weight factor that that node i endows with k when it computes $R_{i,j}$. $w_{i,kj}$ is calculated according to the trust value $\phi_{i,k}$ .On the contrary, $\phi_{i,k}$ is such that i considers k untrustworthy, i will use the deviation test to decide whether accept $F_{k,j}$ as follows:

$$\left|\mathrm{E}(\alpha_k, \beta_k) - \mathrm{E}(\chi_r, \eta_r)\right| < \delta \tag{7}$$

Where δ is a positive constant that represents deviation threshold. If the deviation test turns out negative, $F_{k,j}$ will not be used as a false rating. Else it is incorporated in $R_{i,j}$ using Equation (5) (6). Whether k is considered trustworthy by i or not, the deviation test is always performed and $T_{i,k}$ would be updated according to the test results. In the former case, the deviation test is used only to update $T_{i,k}$; in the latter case, it is used to decide whether to incorporate $F_{k,j}$ in $R_{i,j}$ and update $T_{i,k}$ as well.

d) i and each k will re-evaluate $\theta_{i,j} / \theta_{k,j}$. If $\theta_{i,j} / \theta_{k,j}$ is below t_r , j would be regarded as a misbehaving node by i / k . i / k deactivates j in its routing table and isolates j for a time slice.

e) i sends an error message RERR to the upstream nodes in the route and perform "Local Re-routing" in below section and try to resend the packet.

E. Selective Node Initialized Re-routing

In original ARAN, it is the responsibility of the sender to reinitiate the route discovery again when a misbehaving node is detected in the path. In CSRAN, "Local Re-routing" strategy is adopted to enhance the efficiency. Once misbehaviors of a selfish or malicious node j en route is detected, the previous-hop i who detects will initiate local re-routing destined to D. i re-chooses the next-hop node j^* that has highest reputation from the remaining RREPs for the same RDP packet. Then i stores its information in its sent-table as the path of this data transfer and tries to resend the packet using the new path. This local re-route scheme can reduce the overhead caused by re-routing and is more practical compared to finding a new route from the source to the destination, which is disjoint with the complete old path.

Ⅴ. Performance Analysis and Simulation

The reputation system is key component of the schemes, thus it is necessary to analyze its performance. We adopt a robust and efficient reputation system [5] which make a use of a modified Bayesian procedure to incorporate second-hand information into the first-hand information to enhance the efficiency of system. It introduces a discount factor for past experiences serving as the fading mechanism. To strengthen the robustness of the system, it employs the trust ratings of nodes and to adopt deviation test to detect and avoid false rating. Each node will classify the other neighbor nodes in the networks into trustworthy and untrustworthy according to trust rating. The information from trustworthy nodes would be accepted and the trust value of the node is blemished if the rating is false. False ratings from untrustworthy nodes would be rejected if it could not pass the deviation test. In a word, any malicious action would result in the degradation of its trust value thus malicious nodes can not submit false ratings for others optionally.

Then, we give the analysis of the proposed reputation-based secure routing protocol by discussing different forms of attacks and presenting ways of counteracting them by the introducing reputation-based scheme. Since our scheme is based on ARAN, it is provided with the security property that ARAN guarantees. It can defend against unauthorized participation, spoofed route signaling, fabricated routing messages, alteration of routing messages, replay attacks effectively [11]. Since most of the attacks performed by malicious unauthenticated nodes can be detected and defended against by the use of the secure routing ARAN protocol, we only need to discuss those attacks performed by authenticated misbehaving nodes that the ARAN protocol can not defend against.

Case 1: An authenticated misbehaving node might make a false claim of knowing the route to a destination and generate a RREP for a destination for which it does not have a route. In CSRAN, after receiving the data packet to the corresponding destination, the authenticated selfish node would not receive the DACK from the destination. The previous-hop and the neighbors of this selfish node will give a negative rating to its reputation. Once the reputation of this selfish node falls below the threshold, it will be considered as misbehaving and will eventually be isolated. Thus, this attack can be detected and defended against by our scheme.

Case 2: An authenticated misbehaving node might not reveal that it knows the route to the destination by not replying to or forwarding control packets so that to save its resources. This selfish behavior will not be able to cause damage to the network directly but it would depress the throughput and performance of the network. Our scheme employs the reputation system to help to resist this type of selfish attack. If the packet has originated from a low-reputed node, the packet is assigned lowermost priority and if the packet has originated from a high-reputed node, the current node sends the data packet to the next hop in the route as soon as possible. Hence, these selfish nodes will see a considerable increase in network latency and it would be encouraged to participate and cooperate in the ad hoc network.

Case 3: An authenticated misbehaving node might promise to route data packets, but then it starts to drop all the data packets that it receives. In such a scenario, the previous-hop and neighbors of the node will give it a negative reputation rating and the reputation of the node will be reduced. Eventually, the node will be isolated by its neighbors for a period.

Case 4: An authenticated misbehaving node might drop data packets to decrease the throughput of the mobile ad hoc network continuously. Since in our scheme, the intermediate nodes relay the packets only to highly reputed neighbors, it reduces the risk that nodes will intentionally drop the packet. As a result, the number of packets intentionally dropped is reduced and the throughput of the system rises. In other words, our scheme encourages the node to cooperate in the network.

Case 5: Authenticated selfish nodes might collude by giving positive recommendations to each other so that to increase their reputations. The RARAN [15] prevents this attack by having the nodes rely on their own experience rather than the experience of their peers. However, it would make the reputation system inefficient. In CSRAN, the neighbors share and exchange their first-hand reputation rating to enhance the efficiency. It also employs the trust ratings and deviation test to detect and avoid false rating from colluding or malicious nodes. since only first hand information $F_{i,j}$ is published and the exchange of reputation information only happens among neighboring nodes, thus CSRAN is more efficient than [15]

However, an authenticated well-behaved node might become a bottleneck since in the presented reputation-based scheme the node with the highest reputation is always selected as the next hop by its neighbor. As a result, the nodes with higher reputations will become overloaded, while the other nodes become totally free. This problem is solved in the proposed scheme through the following procedure: when authenticated nodes are congested and they can not fulfill all control packets broadcasted in the MANET, they can choose not to reply to other nodes requests in order to do their own assigned load according to their battery, performance and congestion status.

We implemented our scheme using the network simulator ns-2[7]. For the propagation, we used the two-ray ground reflection model, while the IEEE 802.11 Distributed Coordination Function (DCF) was used at the MAC layer. Nodes had a physical radio range of 250 m and a raw bandwidth of 2 Mbps. We simulated a network of 50 nodes randomly placed in an area of 700×700, where we randomly selected several nodes that misbehave. There are 15 source-destination pairs and each source transmits at a Constant Bit Rate (CBR) of 2 packets, with a packet size of 512 bytes. The simulation time is 900 s, where the time intervals were 60 seconds long.

Figure1 and 2 shows the performance comparisons of in standard DSR [8] and CSRAN (labeled as the trusted DSR). The results indicate that the total number of packets lost with the trusted DSR always lower than that standard DSR despite the increase in misbehaving nodes. This is because misbehaving nodes are detected in time and bypassed during route discoveries. The lower packet loss also helps to maintain a better throughput of the network in the presence of misbehaving nodes. These results accord with our expectations.

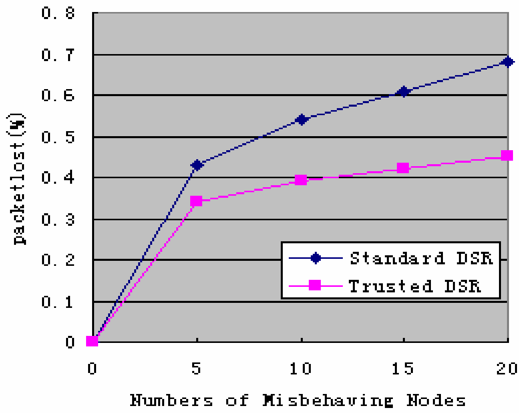

Figure 1: packet loss comparisons of trusted DSR and standard DSR

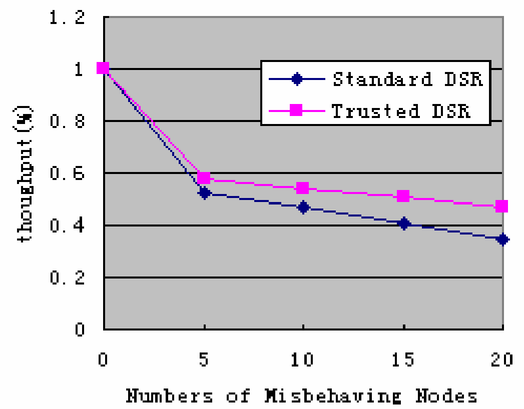

Figure 2: throughput comparisons of trusted DSR and standard DSR

Ⅵ. Conclusion

We have proposed a cooperative secure routing protocol to prevent and detect malicious attacks and selfish behaviors. It is based on ARAN, but it proves to be more efficient and more secure than normal ARAN secure routing protocol in defending against both malicious and authenticated selfish nodes. It adopts a robust and efficient reputation system to help enforce the security and cooperation of the routing protocol. A detailed analysis is given to show our protocol can defend against most of the current attacks and the result of our simulation shows that CSRAN can help to enhance the performance of ad hoc networks. Furthermore, it can also locate the misbehaving node on transmit path.

Acknowledgment

This work is supported by National Natural Science Foundation of China (60502047), Education Bureau of Fujian Province (JA07030), Natural Science Foundation of Fujian Province (2008J0014).

References

[1] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of MOBICOM 2000, pages 255~265, 2000.

[2] Sonja Buchegger and Jean-Yves Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes | Fairness In Dynamic Ad-hoc NeTworks. In Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne,CH, June 2002. IEEE.

[3] Audun Josang and Roslan Ismail. The beta reputation system. In Proceedings of the 15th Bled Electronic Commerce Conference, Bled, Slovenia, June 2002.

[4] Sonja Buchegger and Jean-Yves Le Boudec. The effect of rumor spreading in reputation systems in mobile ad-hoc networks. Wiopt'03, Sofia-Antipolis, March 2003.

[5] Sonja Buchegger, Jean-Yves Le Boudec , "A Robust Reputation System for P2P and Mobile Ad-hoc Networks", In Proceedings of P2PEcon 2004, Harvard University, Cambridge MA, U.S.A., June 2004.

[6] James O. Berger. Statistical Decision Theory and Bayesian Analysis. Springer, second edition edition, 1985.

[7] NS-2: Network Simulator 2. Available at http://www.isi.edu/nsnam/ns/

[8] David Johnson,David Maltz,Hu Yih-Chun.The dynamic source routing protocol for mobile ad hoc networks (DSR)[R].Internet Engineering Task Force(IETF),2003.

[9] R. Molva and P. Michiardi. Security in Ad hoc Networks. Personal Wireless Communication, September 2003, pages 756-775.

[10] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking, September, 2002, pages 12-23.

[11] K. Sanzgiri, B. Dahill, B. Levine, E. Royer and C. Shields. A Secure Routing Protocol for Ad hoc Networks. Proceedings of the tenth IEEE International Conference on Network Protocols, November 2002, pages 78-87.

[12] Y. Hu, D. Johnson, and A. Perrig. SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks. In Fourth IEEE Workshop on Mobile Computing Systems and Applications, June 2002, pages 3-13.

[13] P. Papadimitratos, Z. Haas and P. Samar. The Secure Routing Protocol (SRP) for Ad Hoc Networks. Internet-Draft, draft-papadimitratos-secure-routing-protocol-00.txt, December 2002.

[14] M. Zapata and N. Asokan. Securing Ad Hoc Routing Protocols. In Proceedings of the ACM Workshop on Wireless Security, September 2002, pages 1-10.

[15] Mahmoud A,Sameh A,El-Kassas S. Reputed Authenticated Routing for Ad Hoc Networks Protocol (Reputed-ARAN)[A].Proc of the IEEE Int'l Conf on Mobile Ad Hoc and Sensor Systems[C].2005.787-794.

Zhang Yihui is graduate student in the Department of Math and Computer Science at the Fujian Normal University. She received the B.S degree in the Department of Information and Computer Science from Civil Aviation University of China at 2004.

Her research interests include network protocol design, especially for mobile ad hoc networks and energy concerned sensor networks. Her current research focuses on secure routing and anonymity issues in wireless ad hoc networks. Contact her at Email:zyh_1983@126.com.

Li Xu is a professor in the Department of Math and Computer Science at the Fujian Normal University. He received the B.S and M.S degrees form the Fujian Normal University in 1992 and 2001. He received the Ph.D. degree from the Nanjing University of Posts and Telecommunications in 2004. Now he is the assistant dean of School of Maths and Computer Science and Co-Director of Key Lab of Network Security and cryptography.

He specializes in network protocol design, especially for wireless network. His current research focuses on secure issues in wireless ad hoc networks.

Dr. Xu is the senior member of CCF and CIE in China. He has published over 60 papers. His research group at FJNU has developed Network and Information Security, Complex System and Network, Intelligent Information Processing in Communication Networks, P2P, Grid, and Intelligent Information Processing in Communication Network. Contact him at Email: xuli@fjnu.edu.

Xiaoding Wang is a assistant research in the key lab of security and cryptology of Fujian Normal University. He received the Master degree of Computer Science from Wollongong University of Australia in 2008.

His researches focus on cryptology and network security Contact him at Email: Wangdin1982@yahoo.com.cn.