Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2010, Article ID 258935, 10 pages
doi:10.1155/2010/258935

Research Article

COSR: A Reputation-Based Secure Route Protocol in MANET

Fei Wang,[1] Furong Wang,[1] Benxiong Huang,[1] and Laurence T. Yang[2]

[1] *Electronic and Information Engineering Department, Huazhong University of Science & Technology (HUST), 1037 Luoyu Road, Wuhan 430074, China*
[2] *Department of Computer Science, St. Francis Xavier University, Canada*

Correspondence should be addressed to Fei Wang, wangfei@hust.edu.cn

Received 2 April 2010; Accepted 25 June 2010

Academic Editor: Liang Zhou

Now, the route protocols defined in the Mobile Ad Hoc Network (MANET) are constructed in a common assumption which all nodes contained in such networks are trustworthy and cooperative. Once malicious or selfish nodes exist, all route paths built by these protocols must be broken immediately. According to the secure problems within MANET, this paper proposes Cooperative On-demand Secure Route (COSR), a novel secure source route protocol, against malicious and selfish behaviors. COSR measures node reputation (NR) and route reputation (RR) by contribution, Capability of Forwarding (CoF) and recommendation upon Dynamic Source Route (DSR) and uses RR to balance load to avoid hotpoint. Furthermore, COSR defines path collection algorithm by NR to enhance efficiency of protocol. At last, we verify COSR through GloMoSim. Results show that COSR is secure and stable.

1. Introduction

A mobile Ad Hoc network is a collection of autonomous nodes that communicate with each other. There are no base stations, access points, and any centralized control equipment. The entering and exiting of any node occur freely and without any management. Further, as the wireless transmission range of each individual node is limited, the establishment and maintenance of all route paths in the MANET depend on all other nodes. In this situation, a trustworthy environment is important to Ad Hoc network routing protocol.

Recently, a lot of researches have been done on learning multihop path in the MANET. This body of literature can be categorized into two main groups. (1) Table-Driven Routing Protocols, such as DSDV [1], and OLSR [2]. These protocols maintain a consistent and up-to-date route table to all available destinations at each node. (2) On-Demand Routing Protocols, such as DSR [3], and AODV [4]. These protocols can react well to frequently node mobility and rapid network topology changes, and they are not necessary to maintain all routes periodically.

We focus on on-demand routing protocols, especially DSR. This group of routing protocol has a common assumption that all nodes in an MANET are not malicious nodes and all of them are cooperative. Due to this assumption, misbehavior could destroy route paths established by routing protocol easily. So far, there are some secure routing protocols have been proposed, such as Ariadne [5], SEAD [6], CONFIDANT [7], and CORE [8].

In this paper, we make two contributions to the area of secure routing protocols for MANET. First, we propose a reputation-based secure source routing protocol, called COSR. According to the mobility, self-organization, and secure problems of MANET, node reputation in COSR is both regarded as its trustworthiness and CoF which the node claimed or promised to others. Further, COSR uses route reputation to choose the best route path. Second, we present the simulation of several routing attacks and execute performance evaluation of COSR. Relative to previous schema in reputation-based routing protocol, COSR is more secure and more efficient.

The rest of this paper is organized as follows. Section 2 introduces main secure problems of current routing protocol in the MANET, and Section 3 introduces related work. We present reputation model and routing protocol of COSR in Section 4. Section 5 performs simulation and discusses results. Section 6 provides our conclusion and future work about COSR.

2. Problems

Current MANET routing protocols face a lot of problems, such as security and performance. We will describe them in detail as follows.

(i) *DoS:* Due to the lack of packet certification in route discovery and path collection, attacker would inject a large number of protocol messages with wrong route information. In general, DoS attack can be performed as Route Cache Overflow [9] and Sleep Deprivation Torture [10].

(ii) *Blackhole:* An attacker attracts route paths to pass it by promising the shortest route or service and then drops or forwards data packets to other malicious nodes for mounting more sophisticated attacks. This attack includes two types: *Active Blackhole* and *Passive Blackhole.* Active Blackhole attackers that would inject wrong route information refer to received RREQ or overheard data packets, so that they might attract other nodes to choose them as relay station. On the contrary, Passive Blackhole attackers pose normal nodes during route discovery, and launch attack during data transmitting.

(iii) *Rushing [11]:* This attack targets against on-demand routing protocols. The attacker relays received RREQ without any modification as soon as possible, suppressing any later legitimate RREQ.

(iv) *Wormhole [12]:* Attackers forward RREQ packets by tunneling between attackers to disrupt communication. If a wormhole attacker tunnels all packets through wormhole honestly and reliably, no harm is done.

(v) *Selfish:* In the MANET, nodes own limited resource, especially battery power and bandwidth. Some nodes refuse to forward or selectively forward the packets from other nodes to save its resource.

3. Backgrounds and Related Work

As the MANET is dynamic topology and self-organized, traditional security mechanisms have no effect on routing attack. Hence, a lot of secure routing protocols have been proposed to refer to those attacks. According to their main idea, they can be categorized into four groups.

3.1. Based on Symmetric-Key Encryption. This group uses symmetric-key encryption to enhance the security of routing protocol in the MANET. They mostly apply One-Way Hash function and Hash link algorithm through symmetric key. This primary group includes Ariadne [5], SEAD [6], and SRP [13].

3.2. Based on Asymmetric-Key Encryption. This group uses asymmetric-key encryption to protect routing protocol. They need a trustworthy independent authority, such as Certification Authority (CA). The authority is responsible for creating and publishing certificate for each node. The certificate contains permanent identity and public key. This group just includes ARAN [14].

3.3. Based on Hybrid Encryption. This group uses both of upper encryption technologies. According to the common idea, the fixed part of route message would be signed by private key for integrality. Further, private key also is used to finish node authentication. Furthermore, these protocols use Hash link to protect distance parameter. The representative proposals are SAODV [15] and SLSP [16].

3.4. Based on Reputation. The above protocols use cryptography, authentication, and digital signature to protect security of data contained in the routing messages, and consequently, they enhance security of routing protocols. They belong to the area of hard security [17]. However, the hard security technology can hardly prevent any nodes from malicious or selfish behavior. Further, it also can not promote cooperation among nodes. Hence, reputation is to be implemented in the routing protocol to improve security of routing protocols. The representatives of them are CONFIDENT [7], CORE [8], ASU [13], Watchdog [18], and OCEAN [19].

Table 1 compares the capability of these protocols against above attacks.

4. COSR Protocol

According to such security problems of the MANET, we proposed COSR protocol, a reputation-based secure dynamic source routing protocol. COSR assumes that the link between two nodes is bidirectional, and each node can work in promiscuous mode.

4.1. Protocol Architecture. COSR protocol follows cross-layer design [20]. In the COSR, node's reputation depends on the information from Physical layer, Media Access Control (MAC) layer, and Network layer, and it can be computed by node's CoF, history action, and recommendation. Hence, COSR can be divided into monitor, statistics, reputation model, reputation protocol, and routing protocol. Its architecture is shown in the Figure 1.

(i) MONITOR: This part includes three modules: neighbor monitor, data relay monitor, and CoF monitor. Neighbor monitor works with MAC layer. It is used to monitor neighbors in its radio range and maintain neighbor list. Data relay monitor is placed in the network layer. It requires MAC layer working in promiscuous mode, so that it could check whether the next hop had transmitted its packets. CoF would collect information about capability of forwarding from physical layer and MAC layer, and itincludes node's bandwidth, interface state, mobility status, and power.

Table 1: Comparison of Secure Routing Protocols.

Attacking	Secure Route Protocols										
	ARAN [14]	Ariadne [5]	ASU [13]	CONFIDENT [7]	CORE [8]	OCEAN [19]	SAODV [15]	SEAD [6]	SLSP [16]	SRP [13]	WatchDog [18]
DoS	×	√	√	×	×	×	×	√	√	√	×
Blackhole	×	×	√	√	√	√	×	×	×	×	√
Rushing	√	☆	×	×	×	×	×	×	×	√	×
Wormhole	×	☆	×	×	×	×	×	×	×	×	×
Selfish	×	×	√	√	√	√	×	×	×	×	√

Note: "√"-capable of defending such attack; "×"-cannot defend such attack; "☆"-can be solved with improvement.

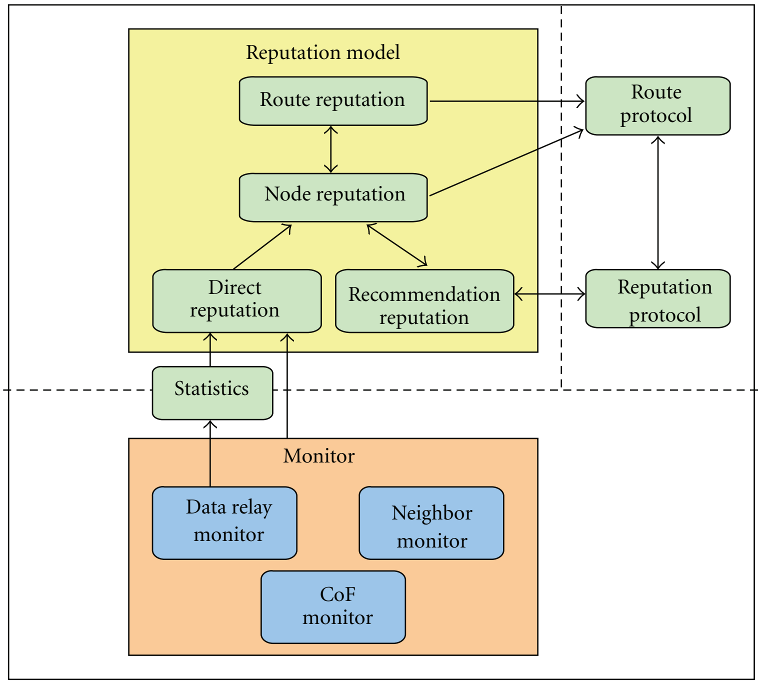


Figure 1: Architecture of COSR protocol.

(ii) STATISTICS: This module is responsible for providing statistics data about neighbors' history behavior. These data include the number of requested and forwarded protocol messages, and data packets.

(iii) REPUTATION model: This is the core module of COSR. It is used to evaluate node's reputation and integrate route reputation relying on the data from MONITOR and STATISTICS.

(iv) Reputation Protocol: This part defines reputation discovery in the MANET. Reputation Protocol clings with routing protocol and uses routing protocol to pigback reputation control message and data.

(v) Routing Protocol: It is an extension of DSR by reputation model. It uses NR and RR to choose the best route path rather than path length. Further, COSR provides a secure mechanism of path collection in route discovery.

4.2. Node Reputation. Firstly, because the COSR uses D-S approach [21] as basic theory to evaluate node's reputation, we introduce the key concept of it simply.

Definition 1. Let Θ be a frame of discernment, $\Theta = \{G, B\}$, where $\{G\}$ means good, $\{B\}$ is contrary, and $\{G, B\}$ represents unknown. If a function $m : 2^{\Theta} \to [0,1]$, where (1) $m(\o) = 0$, and (2) $\sum_{\hat{A}\subset\Theta} m(\hat{A}) = 1$, then m is a basic probability assignment (bpa) over Θ.

In the COSR, *Node Reputation* (*NR*) is defined as a combination of direct reputation, recommendation reputation, and CoF. It is defined as follows:

$$NR_{ij} = R_{\text{direct}}(i,j) \cdot \alpha + R_{\text{rec}}(i,j) \cdot \beta + \text{cof}(j) \cdot \gamma, \tag{1}$$

where NR_{ij} stands for the node reputation value by node N_i on node $N_j \cdot R_{\text{direct}}(i,j)$, and $R_{\text{rec}}(i,j)$ are defined under Θ.

Weights α, β, and γ are the discount factors for different elements of NR, they are defined as follows:

$$\alpha, \beta, \gamma \in [0, 1], \qquad \alpha + \beta + \gamma = 1. \tag{2}$$

4.2.1. Direct Reputation (*R_{direct}*). R_{direct} evaluates the trustworthiness of each next hop neighbor. And, it is a metric of a serial of good, bad and unknown actions. In the COSR, a node seems good that it forwarded all requested protocol messages and data packets. On the contrary, it seems bad. If there are no forwarding requests transmitted to target node, then it is unknown. Further, COSR uses different counters to do statistics of requested and forwarded protocol message and data packet, and received forwarding request. Refer to these counters, packet as metric for control message and byte for data packet. In this method, COSR can prevent some selfish nodes from selectively forwarding short data packets rather than long data packets.

The node reputation contains three parts: $m(\{G\})$, $m(\{B\})$, and $m(\{G, B\})$. They denote trust, distrust, and unknown, respectively, and, they are computed by above counters. Hence, R_{direct} is defined as follows:

$$R_{\text{direct}} = \begin{cases} \dfrac{m(\{G\}) - m(\{B\})}{m(\{G\}) + m(\{G, B\})}, & m(\{G\}) > m(\{B\}), \\ 0, & \text{others}. \end{cases} \tag{3}$$

4.2.2. Recommendation Reputation (*R_{rec}*). R_{rec} represents others' subjective evaluation according to target's behavior, cooperation, and so forth. Therefore, it is a combination of a lot of recommendations from neighbors. In the COSR, a recommendation is defined as follows:

$$\text{Rec} = \langle m(\{G\}), m(\{B\}), m(\{G, B\}) \rangle. \tag{4}$$

A recommendation is originated from direct reputation and subjective view about target node. In the COSR, a recommendation is a basic probability assignment of Θ, and COSR uses D-S formula to combine all received recommendation. Hence, the metric of R_{rec} is defined as the following formula:

$$R_{\text{rec}} = \begin{cases} m(\{G\}) - m(\{B\}), & m(\{G\}) > m(\{B\}), \\ 0, & \text{others..} \end{cases} \tag{5}$$

4.2.3. Capability of Forwarding (CoF). CoF denotes the capability of forwarding packets of a certain node. Simply, we use the remained power, bandwidth, and mobility state to evaluate it. In the CoF, remained power and bandwidth are mandatory, however, mobility state is optional. Only when the node supports Global Positioning System (GPS), it should provide mobility state and its velocity.

As the information of CoF is provided by its owner, malicious node might cheat others by false data. To avoid the emergence of such malicious behavior, COSR takes the following strategies. (1) *Discounting*. COSR uses node's reputation to discount those providing CoF data. (2) *Punishment*. Once COSR finds that any node provided a false CoF, it will punish such node through reducing its reputation level.

4.3. Route Reputation. As the metric of the best route in traditional routing protocols does not concern security, data transmitting must fail when a route path contained one or more malicious nodes. Hence, to avoid such phenomenon, COSR uses two metrics, hops, and intermediate nodes' reputation, and then, we define Route Reputation as the metric of the best route path.

In the COSR, Route Reputation of $\{N_i \rightarrow N_{k1} \rightarrow N_{k2} \rightarrow \cdots \rightarrow N_{km} \rightarrow N_{km} + 1 \rightarrow N_j\}$ is defined by

$$RR_{ij} = \begin{cases} NR_{ik_i} \times \cdots \times NR_{k_{n-1}k_n}, & \forall NR_{k_l k_m} \geq 0, \\ -1, & \text{other}, \end{cases} \tag{6}$$

where $N_{k_1}, N_{k_2}, \ldots, N_{k_{m+1}}$ are the intermediate nodes. The *RR* is composed of *NR* of all intermediate nodes in a certain route path. As *NR* is a real number between 0 and 1, when such route contained more intermediate nodes, its *RR* would be lower even if it closes 1. Hence, shorter route path gains higher *RR*, if there are no malicious nodes. However, if there are malicious nodes in any short route, the *RR* of such route must be lower than a secure longer route. Therefore, *RR* gives attention to both of efficiency and security of route path.

Further, according to formula (6), *NR* is independent of *RR*. In other words, any node can earn higher reputation even if it is included by a route with lower reputation. Hence, COSR does not like [13] that penalizes such nodes around a malicious node.

4.4. Recommendation Game (RG). As direct observation about a strange node mostly is limited even not existent, many solutions (such as CONFIDANT [7], CORE [8], and COSR) use second-hand evaluation to accelerate collecting evidence. However, a malicious node may be described as a perfect node through unfair positive recommendation, and then they can easily inject wrong route into network and launch attacks. Consequently, unfair or false recommendation can break down the constructed reputation system easily. Therefore, we provide a novel mechanism, *recommendation game*, against false recommendation.

4.4.1. Framework

Assumption 1. All nodes in the MANET are rational.

In the recommendation game, there are two kinds of players (node): reputation requester and provider. No matter what reputation requester or provider are, they both deal with reputation request and recommendation rationally. To formulate the recommendation game, we now give its definition.

Definition 2. Let RG be a Recommendation Game: RG = $\{I, A, T, P, U\}$, where I is the set of mobile nodes (reputation requester and providers); $A = \{A_i\}$, where A_i is the action space of node $i \in I$; $T = \{T_i\}$, where T_i is the type space of node i; $P = \{p_i\}$, where p_i is a belief of other players' type based on the type of node i; $U = \{u_i\}$, where u_i is the payoff function for node i.

Table 2: Payoff table of recommendation game.

		Reputation provider		
		Truth	No comment	Lie
Reputation Requester	Trust	S, t	$0, 0$	$S, -l$
	Distrust	$-S, t$	$0, 0$	$-S, -l$

According to the definition, recommendation game has the following properties.

Property 1. Recommendation game is an n-player game, where $n \geq 2$.

In the node set I, there are only one reputation requester and at least one provider. If there is no reputation provider, then this game cannot be played.

Property 2. Recommendation game is an incomplete information game.

Firstly, a requester contained in an RG does not know if a provider is lying. Secondary, requester does not know the relationship between a given provider and the target, while providers know whether the target is their confederate or not. At last, reputation provider does not know whether the requester would trust it or not, and it also does not know how the requester evaluates a recommendation.

Definition 3. Let A_r and A_p^i be action spaces of reputation requester and reputation provider, respectively, then the action spaces are defined by

$$\begin{aligned} A_r &= \{\text{Trust}, \text{Distrust}\}, \\ A_p^i &= \{\text{Lie}, \text{Truth}, \text{No-Comment}\}, \quad i \in I. \end{aligned} \tag{7}$$

Definition 4. Let T_r and T_p be type spaces of reputation requester and reputation provider, respectively. Given a pair of independent constant parameters TC_r and TC_p, where $TC_r, TC_p \in (0, +\infty)$, we can define their type spaces as follows:

$$T_r = [0,\ TC_r], \qquad T_p = \left[0,\ TC_p\right]. \tag{8}$$

Definition 5. Let p_r and p_p be belief of reputation requester and reputation provider, respectively, they are defined as

$$p_r\left(t_p\right) = \frac{1}{TC_p}, \qquad p_p(t_r) = \frac{1}{TC_r}, \tag{9}$$

where t_r and t_p are private information of reputation requester and reputation provider, respectively, and $t_r \in T_r$, $t_p \in T_p$. Both of them are random variables and follow uniform distribution in their type spaces.

4.4.2. Strategy and Payoff. The strategy of reputation requester and provider can be shown in Table 2.

If reputation provider gives a fair recommendation, no matter the requester believes or not, it could gain positive payoff, namely t. However, if it cheats the requester, then it would be denoted as malicious node. And then, such provider would lose others' trust in the later transactions. According to the requester's strategy, "Tit for Tat", it would gain a negative reputation, namely $-l$. t, and l, both are positive parameters and t is less than l commonly. It means that it is more difficult to build reputation and easier to destroy it.

On the other hand, if the requester trusts a lie, then the related attacks *maybe* come true. Consequently, the requester would gain negative payoff about data transmitting. On the contrary, it might obtain a positive payoff for distrusting a lie.

Theory 1. Recommendation requester does not have the absolute best strategy.

The strategy of recommendation requester depends on the evaluation of private information about recommendation provider, hence, it does not have the absolute best strategy. In other words, recommendation requester has the risk of the final strategy for ever.

Theory 2. The recommendation provider conditional makes "TRUTH" as it is the absolute best strategy, and the condition is defined as

$$TC_p < (t + l). \tag{10}$$

Equation (10) is the design reference about parameters of RG. We can choose appropriate t and l according to the detail application scenario, to make recommendation provider has only one strategy, TRUTH, and then, unfair positive recommendation should be reduced sharply.

4.5. Reputation in Route Discovery. Routing protocol in the COSR is based on DSR, hence, route discovery of COSR contains two mechanisms which are shown in Figure 2.

4.5.1. RREQ and RREP. RREQ and RREP are basic methods to discover route paths, however, they only can obtain limited route paths which are shown as white blocks in Figure 2(b). In this procedure, malicious nodes may launch attack in two cases: broadcasting wrong RREQ and transmitting false RREP. The possible attacks include DoS, Blackhole, and selfish. Due to this problem, COSR uses reputation against such attacks. When a node received an RREQ or RREP packet, it should check the sender's reputation, firstly. If sender's reputation does not refer enough to reputation threshold, such node would not believe route information contained in received packet and would abort it without any notification.

4.5.2. Path Collection. Path collection is an extended mechanism to discover more route paths in only one procedure of RREQ and RREP. Path collection includes two directions: forwarding and reversing. Firstly, forwarding direction only allows source node and intermediate nodes collect route paths along the direction to destination contained in RREP.

Table 3: Simulator parameters

Dimensions of Space	1000 m × 1000 m
Total Number of Nodes	40
Node Placement	Uniform
Mobility	Random Waypoint Model
Move Speed	0~20 m/s
Mobile Pause Time	0s
Max Transmission Range	250 m
MAC	802.11
Link Bandwidth	2 Mbps
Application	30 CBR Connections, 64 B/packet, 1 packet/s
Simulation Time	900 s
Payoff Parameters of RG	$\alpha = 0.3, \beta = 1.0$

It is shown as lightgreen blocks in Figure 2(b). Secondary, reverse direction permits all nodes related to this route discovery to collect reverse route paths to upriver nodes. It is shown as lightcyan blocks in Figure 2(a). Obviously, path collection could accelerate route discovering. However, it still has to face a serial of malicious attacks, such as DoS, Blackhole, and selfish, because relative packets and route information were not certificated. Similarly, COSR uses reputation of packets' sender to verify whether to believe or not.

5. Evaluation of COSR

5.1. Environment. The evaluation of COSR is performed upon the GloMoSim, a simulator for wireless network. In the GloMoSim, we configure a mobile Ad Hoc network with a number of connections. Each experiment was repeated FIVE times with different seed which is a parameter configured in the GloMoSim and affects placement and movement of nodes. The main parameters of environment are listed in Table 3.

5.2. Scenario. The evaluation would be done at following scenarios.

(i) *Blackhole*: This attack includes active Blackhole (ABH) and passive Blackhole (PBH). Attackers would drop all data packets which need forwarding. Blackhole attackers would never initiate a CBR connection. Active Blackhole attacker will actively sniff neighbors' RREQ and inject RREP with false route path. Passive Blackhole attackers guise normal nodes in the route discovery, but they pose blackhole in the data transmission.

(ii) *Selfish:* Selfish nodes discard data packets selectively according to preconfigured probability.

(iii) *DoS:* Attackers would inject various protocol messages with wrong and long route, including RREQ, and RREP. Once attack is running, attacker would not participate in any application.

Table 4: The comparison of ratio of packet received

		Attacks			
		ABH	PBH	Selfish	DoS
Protocols	COSR	79%	76%	82%	69%
	DSR	34%	42%	76%	61%
	CONFIDENT without Configured Friends	40%	52%	77%	45%
	CONFIDENT with Configured Friends	76%	80%	85%	77%

5.3. Performance Metrics

(i) *Average Path Length (APL):* This is defined as the average hop number of delivered data packets between sources and destinations. It denotes end-to-end delay.

(ii) *Percentage of Packet Received (PPR):* This is defined as the ratio of the number of data packets received by the destinations to all sent by the source nodes. PPR not only shows the throughput of routing protocol, but also reflects the security and reliability of it.

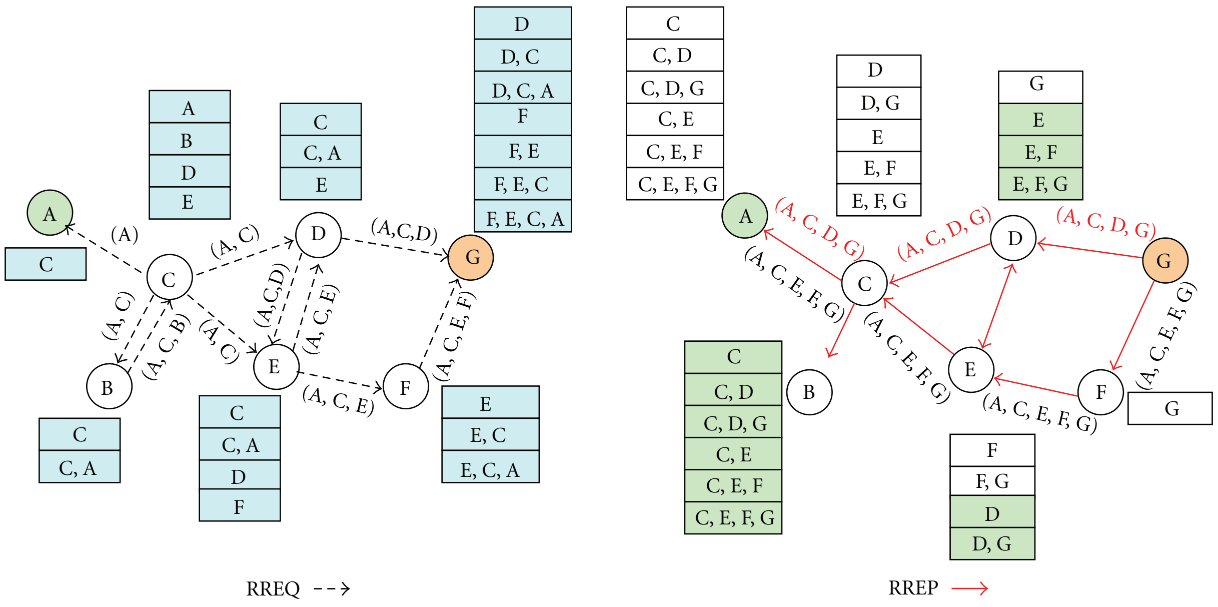
(iii) *Normalized Protocol Load (NPL):* This is defined as the ratio of the number of originated control messages to the number of delivered data packets. NPL describes the efficiency of routing protocol.

5.4. Results and Discussing

5.4.1. Varying Proportion of Blackhole and Selfish Nodes. Figure 3 shows the capability of COSR against Blackhole and selfish attack. According to the result, COSR improves the PPR largely contrasts with DSR on both active Blackhole and passive Blackhole. Due to lack of any security mechanism, DSR's PPR drops down sharply and only 20% of data packets are delivered successfully at the worst situation. On the Contrary, COSR can maintain PPR to be about 50% even 90% of nodes are malicious. The result of selfish attack is similar to Blackhole.

5.4.2. Varying Proportion of DoS Nodes. Figure 4 shows the capability of COSR against DoS attack. The result shows that DSR's PPR decreases sharply with the growing of the ratio of rushing attacker. Due to injecting a large number of wrong route information by DoS attacker, mostly nodes' route cache within DSR would overflow rapidly. At the worst situation, less than 10% of data packets can be delivered successfully. However, COSR plays better and its PPR is much smoother than DSR's.

5.4.3. Varying Proportion of Liars. As recommendation is the main element of reputation, false recommendation produced by liars may destroy reputation system. Figure 5 verifies the capability of COSR against lies. This experiment is to be done at the situations in which the network contains 5% active Blackhole attackers. Further, all liars are selfish. The result shows how many data packets are delivered when there are liars in the MANET for two scenarios: COSR without RG



(a) Propagation of RREQ

(b) Propagation of RREP

Figure 2: Route discovery and path collection in COSR.

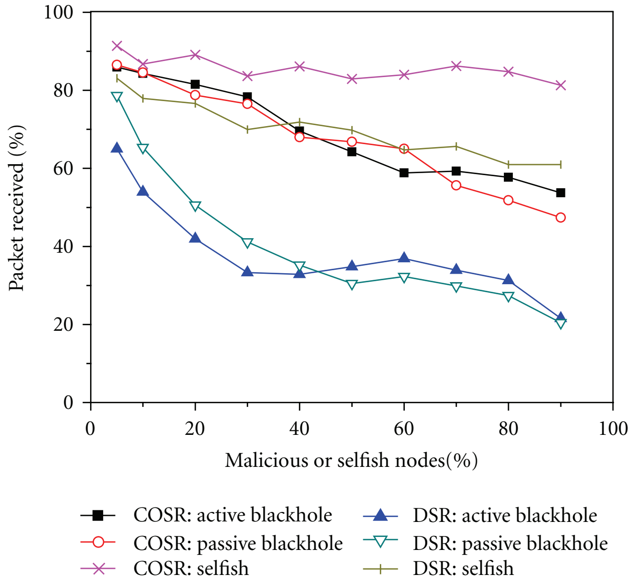


Figure 3: COSR against blackhole and selfish.

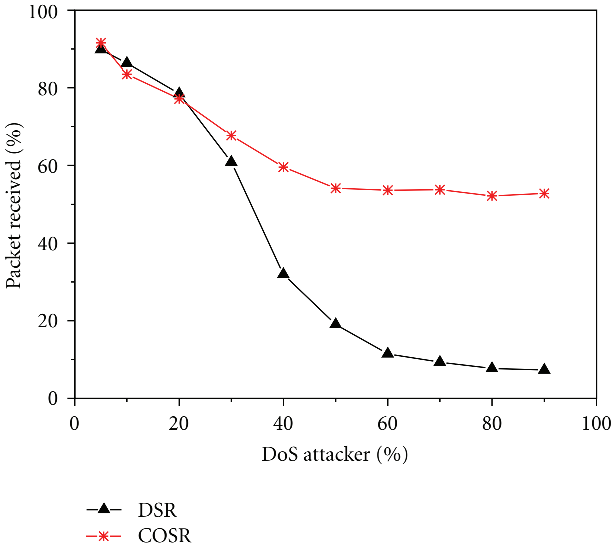


Figure 4: COSR against DoS.

and COSR with RG. By contrasting Figure 5 with Figures 3 and 4, it can be found that lies could influence the effect of reputation model of COSR, but when RG begins work, its PPR is improved obviously.

5.4.4. Performance. These experiments are done at the environment, that there are 30% of nodes are malicious, and they are done at three scenarios: active Blackhole, passive Balckhole, and selfish.

In the Figure 6, with the growing of pause time, NPL is decreased continually, because longer pause time makes topology of network stabler. By contrasting COSR with DSR, NPL of COSR is larger than that of DSR, especially when pause time is small. On the contrary, their NPLs are close when topology of network is changing slowly. Figure 7 shows the NPL of COSR and DSR with the growing of maximum velocity. It is the same as Figure 6, NPL of COSR is larger than that of DSR when topology of network is changing fast.

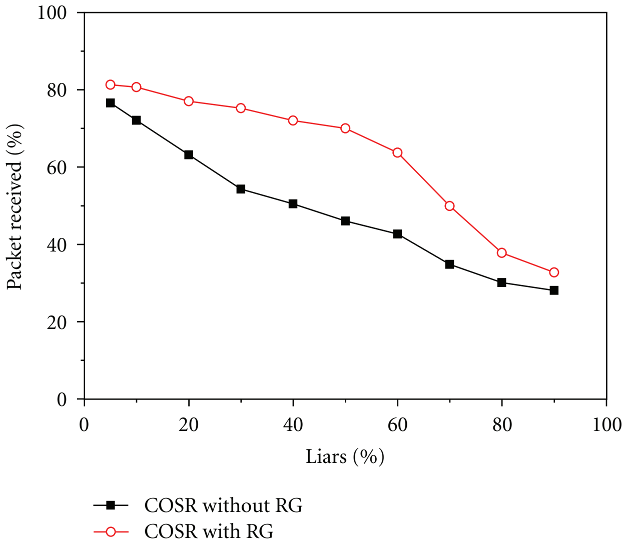


Figure 5: COSR against Liars.

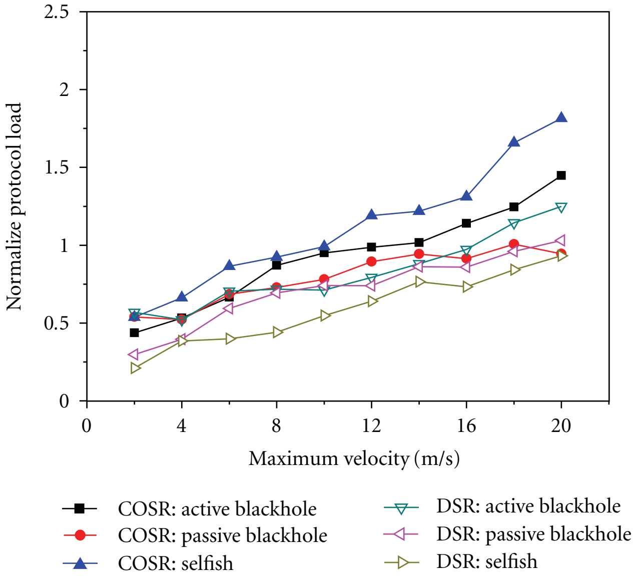


Figure 7: NPL of COSR and DSR with various maximum velocity.

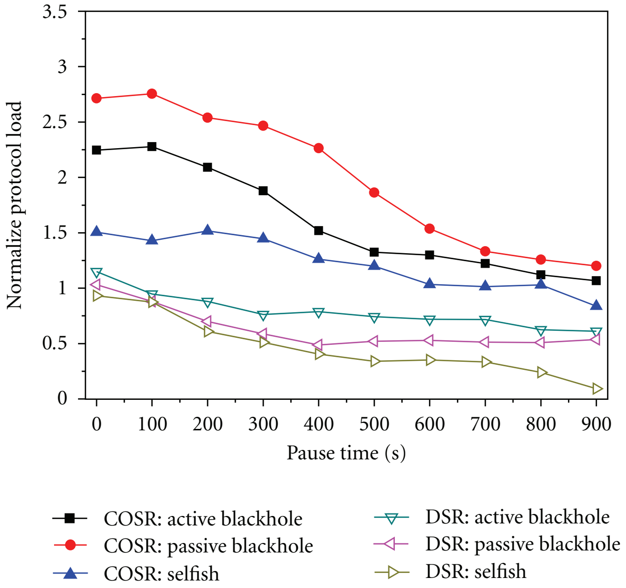


Figure 6: NPL of COSR and DSR with various pause time.

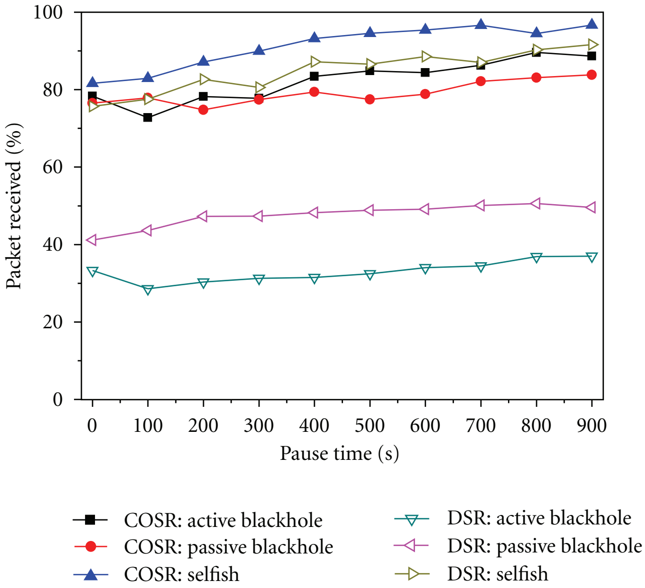


Figure 8: Throughput of COSR and DSR with various pause time.

Figures 8 and 9 show the throughput of COSR and DSR with such scenarios. According to the results, COSR gains higher throughput than DSR, even topology of network is changing fast. As active Blackhole attacker performs more active malicious behavior so that COSR could detect it easier than passive Blackhole, though active Blackhole is more aggressive than passive Blackhole in DSR.

Figures 10 and 11 give the end-to-end delay of data packets. With various pause time, APL of COSR is less than that of DSR greatly. However, their APLs are closed with various maximum velocity. This shows that pause time is more important on affecting network topology than mobile velocity. With growing pause time, the difference becomes significant because fixed network topology is more conducive to COSR detecting malicious nodes.

5.4.5. Comparison. Moreover, we do a comparison simulation among COSR, DSR, and CONFIDENT within the scenario which is described by Table 3 and contained 30% malicious nodes. According to CONFIDENT, we provide two sets of simulation result. In the first set, CONFIDENT does not contain preconfigured friends list. In the other set, we configure several default friends in each node’s Trust Manager before simulation according to CONFIDENT’s design. In this comparison simulation, we mainy compare the ratio of packet received when the routing protocol is against active Blackhole, passive Blackhole, Selfish, and DoS.

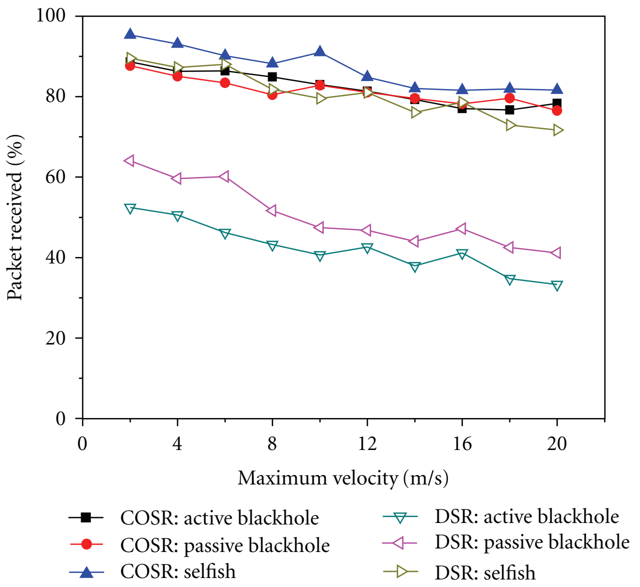


Figure 9: Throughput of COSR and DSR with various maximum velocity.

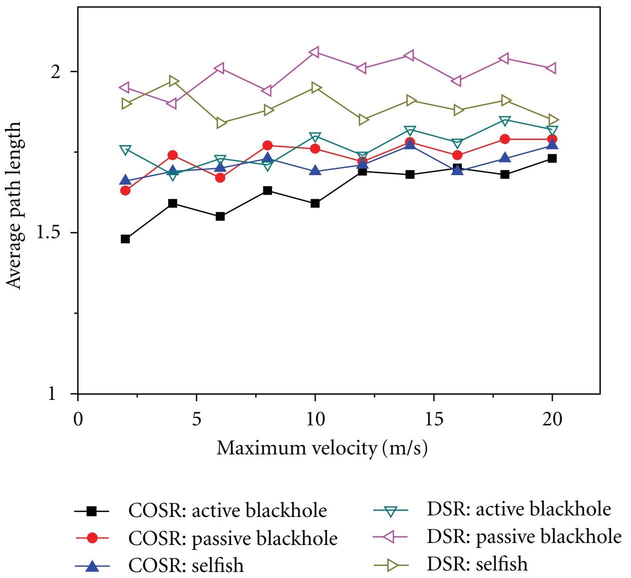


Figure 11: APL of COSR and DSR with various maximum velocity.

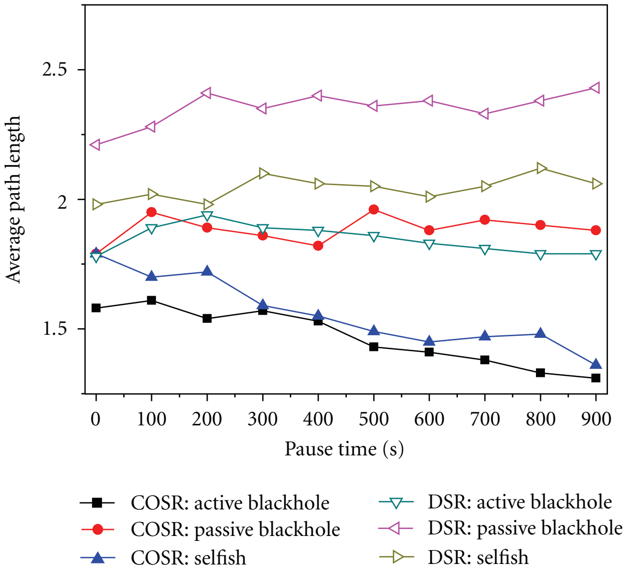


Figure 10: APL of COSR and DSR with various pause time.

According to the simulation result shown in Table 4, we can find that CONFIDENT gains the highest performance when it contains preconfigured friends. However, CONFIDENT's performance decreases sharply when we canceled the preconfigured friends. At this situation, CONFIDENT is similar to DSR, on the contrary, COSR acquires satisfactory performance. The reason is that COSR designed a dynamical mechanism to construct friendship between strange nodes in the SON, but CONFIDENT does not provide such scheme. Therefore, COSR is more suitable for the dynamical SON in which there are a lot of nodes joining and leaving continuously.

6. Conclusion

By using dynamic source routing protocol, communication among self-organized wireless network comes true. However, the existing malicious nodes destroyed the traditional routing protocol, such as DSR, and AODV. To mitigate the effect of malicious behavior, we present a reputation-based secure routing protocol, called COSR, for MANET. The COSR uses a novel reputation model to detect malicious and selfish nodes and make all nodes more cooperative. Further, reputation is not only used to evaluate the trustworthiness of any node, but also to describe its CoF. Due to such design, COSR can protect network against the primary routing attacks and balance load on all secure route paths to avoid *hotpoint* and enlarge throughput of whole network consequently. Under most simulation scenarios, COSR improves PPR, and APL largely refers to DSR, though NPL of COSR is more than that of DSR. Therefore, the ongoing research of COSR is improving is efficiency of COSR. We hope to decrease its NPL with current PPR and APL levels.

Acknowledgment

This work was supported by Program for new Century Excellent Talents in University (NCET-06-0642).

References

[1] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing(DSDV) for mobile computers," in *Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM '94)*, pp. 234–244, ACM Press, London, UK, August-September 1994.

[2] T. Clausen, P. Jacquet, A. Laouiti, et al., "Optimized link state routing protocol," Internet-Draft, draft-ietf-manet-olsr-05.txt, October 2001.

[3] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*, chapter 5, pp. 153–181, Kluwer Academic Publishers, Dodrecht, The Netherlands, 1996.

[4] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop Mobile Computing Systems and Applications (WMCSA '99)*, pp. 90–100, IEEE Press, 1999.

[5] 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*, pp. 12–23, September 2002.

[6] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications*, IEEE, June 2002.

[7] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol (cooperation of nodes: fairness in dynamic ad-hoc networks)," in *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC '02)*, pp. 226–236, ACM Press, June 2002.

[8] R. M. P. Michiardi, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proceedings of the 6th Joint Working Conference on Communications and Multimedia Security*, pp. 107–121, IEEE, December 2002.

[9] J. Lundberg, "Routing Security in Ad Hoc Networks," http://citeseer.ist.psu.edu/400961.html.

[10] F. Stajano and R. Anderson, "The resurrecting duckling: security issues for ad hoc wireless networks," in *Proceedings of the 7th International Workshop on Security Protocols*, pp. 172–194, Cambridge, UK, April 1999.

[11] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in *Proceedings of the ACM Workshop on Wireless Security*, pp. 30–40, ACM, September 2003.

[12] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies*, vol. 3, pp. 1976–1986, San Francisco, Calif, USA, March-April 2003.

[13] P. Dewan, P. Dasgupta, and A. Bhattacharya, "On using reputations in ad hoc networks to counter malicious nodes," in *Proceedings of the 10th International Conference on Parallel and Distributed Systems (ICPADS '04)*, pp. 665–672, Newport Beach, Calif, USA, July 2004.

[14] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," Tech. Rep. 01-37, Department of Computer Science, University of Massachusetts, August 2001.

[15] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of ACM Workshop on Wireless Security*, pp. 1–10, ACM Press, September 2002.

[16] P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," in *Proceedings of IEEE Workshop on Security and Assurance in Ad Hoc Networks*, pp. 27–31, IEEE, 2003.

[17] L. Rasmusson and S. Janssen, "Simulated social control for secure internet commerce," in *Proceedings of the New Security Paradigms Workshop*, ACM, 1996.

[18] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM '00)*, pp. 255–265, Boston, Mass, USA, August 2000.

[19] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," Research Report cs. NI/0307012, Standford University, 2003.

[20] M. Conti, G. Maselli, G. Turi, and S. Giordano, "Cross-layering in mobile ad hoc network design," *Computer*, vol. 37, no. 2, pp. 48–51, 2004.

[21] G. Shafer, *A Mathematical Thoery of Evidence*, Princeton University Press, Princeton, NJ, USA, 1976.