International Journal of Security and Its Applications
Vol. 10, No. 7 (2016) pp.333-344
http://dx.doi.org/10.14257/ijsia.2016.10.7.29

# A New Authentication Solution for Prevention of Some Typical Attacks in Ad Hoc Network

Haiyan Liu[a,*] and Kongjun Bao[b]

*Engineering Training Center, Zhengzhou University of Light Industry, Zhengzhou, 450002, China*
*[a]2003056@zzuli.edu.cn, [b]baokongjun@zzuli.edu.cn*

## *Abstract*

*Ad Hoc network is a multi-hop temporary communication network of mobile nodes. Because the lack of infrastructure support in Ad Hoc network, some attacks are more serious than in other type of networks.* [1] *Therefore security problem in this type of network is a challenging issue. To against the attacks which threat seriously security of Ad Hoc network, a new authentication scheme is proposed. The proposed solution involves three main stages: intermediate nodes pre-authenticating stage, common key $k_i$ between $n_0$ and $n_i$ negotiating stage and authentication during all routing phases. At the same time, the network simulation of the proposed solution is conducted. The simulation result shows that the proposed solution effectively resists the attacks mentioned above. Meanwhile, the negative affection to the performance of network, such as delay and overheads, is tolerable according to the simulative result. The research in this paper enable us to put forward a reasonable authentication solution during all phases.*

***Keywords****: Ad Hoc Network masquerade attack, authentication solution*

## 1. Introduction

For the lack of infrastructure support in Ad Hoc network, such network is more available. Security in mobile ad hoc networks is difficult to achieve. [2] This network is suitable for applications in military battle field, emergency rescue, vehicular communications, mining operations and so on. Ad Hoc Network transmits information by nodes cooperating with each other. All the nodes in this network are movable and the topology of the network is changing dynamically.

A new authentication solution is presented in this paper. The proposed scheme involves three main stages: intermediate nodes pre-authenticating stage, common key $k_i$ between $n_0$ and $n_i$ negotiating stage and authentication during all routing phases. The network performance used proposed scheme is proved fine through experiment in the section 5.The additional delay and overheads caused by proposed solution is tolerable according to the simulative result.

The remainder of this paper is organized as follows: Section 2 briefly presents the related background knowledge, the two main known routing protocols and the main types of the attacks in Ad Hoc network. The related work on research against some typical attacks in Ad Hoc Network is summarized in Section 3. A new authentication scheme is proposed in section 4. We analyze and discuss simulation results in Section 5. Finally, the paper is concluded in Section 6.

[*] Corresponding Author

ISSN: 1738-9976 IJSIA

## 2. Knowledge on Routing Proposal and Attacks

In Ad Hoc Network, some routing protocols have been employed extensively in the real communication, among which AODV(Ad Hoc On-demand Distance Vector) and DSR(Dynamic Source Routing) are the two most popular protocol adopted in Ad Hoc Network. These two protocols are discussed as follows.

### 2.1. Protocols in Ad Hoc Network

- **AODV Protocol**

AODV routing protocol is Ad Hoc On-demand Distance Vector's abbreviation, It is designed for networks of tens to thousands of mobile nodes. AODV can handle low, moderate, and relatively high mobility rates, as well as a variety of data traffic levels. Route discovery is not started until it is required. The protocol operates in two mechanisms: route discovery and route maintenance.

One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes.

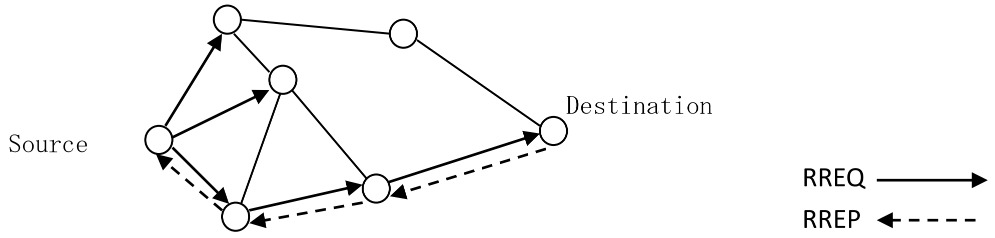


**Figure 1. Establishing a New Route based on AODV Protocol**

In AODV protocol, as illustrated in Figure 1, source node broadcasts a Routerequest packet into the network when needed. A node receives a fresh Routerequest will check its RT to see whether it has a route to the requested destination. It replies if there is one, otherwise, the RouteRequest is forwarded. Before forwarding, it keeps a reverse path to the source node in its RT. The RT records the route information of the next hop, the distance and the current highest sequence number it has seen. [3]

Route maintenance starts when topology changes in the network It is used to notify the source node or to trigger a new route discovery. When a link break in an active route is detected, a RERR message is used to notify other nodes that the loss of that link has occurred. [4] The RERR message indicates those destinations which are no longer reachable by way of the broken link.

- **DSR protocol**

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. The protocol consists of the two main mechanisms, "Route Discovery" and "Route Maintenance", [5]which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network.

The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets, for example, for use in load balancing or for increased robustness. Other advantages of the DSR protocol include easily guaranteed loop-free routing, operation in networks containing unidirectional links, use of only "soft state" in routing, and very rapid recovery when routes in the network change. [6]

### 2.2. Typical Types of the Attacks in Ad Hoc Network

For the characteristics of Mobile Ad Hoc Network, it is more vulnerable to various attacks compared with other network. The general attacks in this network involve: masquerade attack, replay attack, alteration of messages, black hole attack, gray hole attack and so on. In this paper, we focuses on the three representative attacks, masquerade attack, replay attack, black hole attack which are resisted by the proposed scheme.

- **Masquerade Attack**

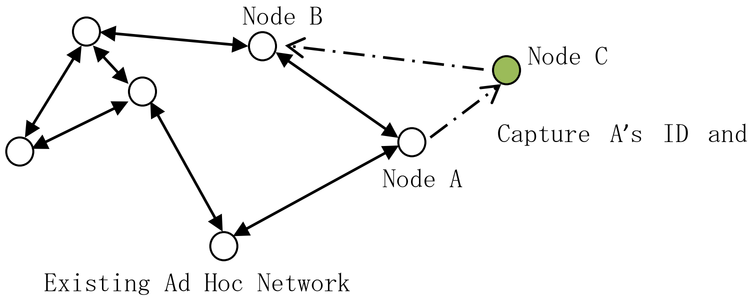


**Figure 2. Masquerade Attack**

Masquerade attack is caused when an unauthorized entity pretends to be another entity. As shown in Figure 2, node C might pose as node A send a message to node B. Node B might be led to believe that the message indeed came from node A. Because usually some other forms of attacks are also embedded. As an instance, node C may capture node A's ID and private key. Later, those details can be replayed to gain illegal access to the network.

- **Replay Attack**

In a replay attack, a user captures a sequence of events or some data units and resends them. For instance, as illustrated in Figure 2, node C launched a replay attack at the same time. For another example, suppose user A wants to transfer some amount to user C's bank account. Both users A and C have accounts with bank B. User A might send an electronic message to bank B, requesting for the funds transfer. User C could capture this message and send a second copy of the same to bank B. Bank B would have no idea that this is an unauthorized message and would treat this as a second and different, funds transfer request from user A. Therefore, user C would get the benefit of the funds transfer twice: once authorized, once through a replay attack.

- **Black Hole Attack in AODV:**

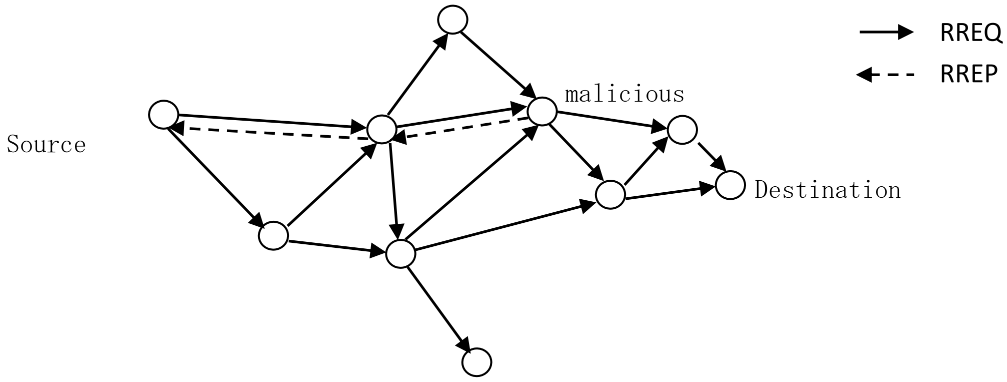


**Figure 3. The Process of the Black Hole Attack**

Black hole attack in AODV protocol is the misbehavior that the malicious node discards the packets. When the source node wishes to communicate with the destination node, illustrated in Figure 3, if there is no route available, it will initiate the routing discovery process in which the source node will flooding RREQ. When the other nodes receives a RREQ during the route discovery phase it replies to the source node with RREP. Eventually the source node will judge which one will be the best route for sending the data to the destination. During this process, a malicious node sends a forged RREP packet to a source node by which the malicious node advertises that it is the destination or the shortest route. Subsequently, the data traffic will flow toward the attacker and source and destination nodes became unable to communicate with each other. Even more seriously, the malicious node will drop the packets. At last, the function of entire network can't work normally.[7]

In this kind of attack, the invader only cause the loss of packets but does not inject any additional packets into the network or alter the current message. Thus the damage of black hole attack is limited comparatively. However the malicious node tries to attract the message from all neighboring nodes to it by means of replies to them as if it is the shortest route to the destination. Compared with traditional selfish behavior known as passive black hole, active black hole can attract a wider range of its neighboring nodes and have severe influence on the success rate of data communication.

## 3. Related Work

The attacks mentioned above causes a serious damage in Ad Hoc Network. To cope with these attacks, many solutions have been presented.

In [7], Ms.Nidhi Sha and rma Mr.Alok Sharma analyze black hole attack in MANET and present two possible solutions. Then they compares the presented solutions to the original AODV depending on the pause time at a minimum cost of the delay in the networks. In [8], authors propose the watchdog and pathrater mechanism to mitigate the dropping packets misbehavior. The watchdog solution belongs to a kind of IDS(Invasive Detection System). It's principle is that each node monitors its successor after sending a packet to it, by overhearing the channel and checking whether it relays or drops the packet. The pathrater accuses a monitored node for misbehaving if this latter drops more than a given number of packets. In [9], authors propose a monitoring approach that overcomes some of watchdog's shortcomings. In this solution, each node monitors its successor and an authenticated 2-hop ACK is used to acknowledge received messages. In

[10], a new routing security scheme based on the reputation evaluation in hierarchical ad hoc networks is proposed. The reputation relation is built based on the behaviors and correlation of the node. It has the incentive mechanism to promote the cooperation of cluster members for forwarding data packets and to increase the activity probability of cluster members in the network. Karlof and Wagner [11] first proposed selective forwarding attacks and suggested that multi path forwarding can be used to counter these attacks in sensor networks. However, the algorithm fails to suggest a method to detect and isolate the attackers from the network. Authors in [12] suggest a modular solution structured around five modules: first is a monitoring module to control packets forwarding, second module detects monitored nodes misbehavior, third one isolates the detected misbehaving nodes whereas fourth module investigates accusations before testifying whether the node has not enough experience with the accused and the fifth module responds to witness requests of the isolator. In [13] channel aware detection (CAD) approach has been proposed that adopts two strategies, hop-by-hop loss observation and traffic overhearing. Each intermediate node in the forwarding path observes the behavior of its previous-hop and next-hop neighbors to detect the misbehaving nodes. These nodes judge the behavior of its neighbors by comparing the observations against two detection thresholds known as monitoring and loss rate threshold. In [14], Hongsong *et. al.,* propose an intrusion detection model to combat the black hole in AODV. In this model, a security agent is used to detect attacks that exploit the route request (RREQ) and the route reply (RREP) packets. The agent monitors RREQ and RREP packets at real-time. If any detection rule is violated, the black hole is detected and blacklisted.

## 4. A New Authentication Solution

A new authentication soluton which can greatly mitigate the typical attacks is proposed in this section.

### 4.1. Some Assumptions and Definitions

1. Key pair ($p_{kni}$ ,$k_{pri}$)between $n_i$ and CA have been existed,which is generated in the procedure of $n_i$ entering Ad Hoc Network .This procedure is not discussed in this paper.

2. The number of the communication route from source node n0 to destination node $n_{m-1}$ is denoted by m, where $n_i$ (i=0,1,2,3,…,m-1)represent the set of nodes constituting the routing path.

3. Each node’s identity is denoted by $ID_i$ which is stored in a table of CA.

### 4.2. The Detailed Procedure of the Solution

The proposed new solution consists of three main stages: intermediate nodes pre-authenticating stage, common key $k_i$ between $n_0$ and $n_i$ negotiating stage and authentication during all routing phases stage. In this section, the solution will be described.

The solution is executed after the routing path seeking procedure, in other words, the one or several route from source node to destination node has been found out. The function of proposed scheme is authenticating the security of existed routing path further.

It is noted that the relationship of stage 1 and stage 2 is really very tight though the procedure is divided into two in theory. $N_0$ receives the Authentication response form CA in the end of stage 1 and will compute common key $k_i$ immediately if the authentication of $n_i$ is successful. For this reason, we will discuss the stage 1 and stage 2 together.

The proposed scheme is shown in Figure 4. The interaction procedure is as follows.

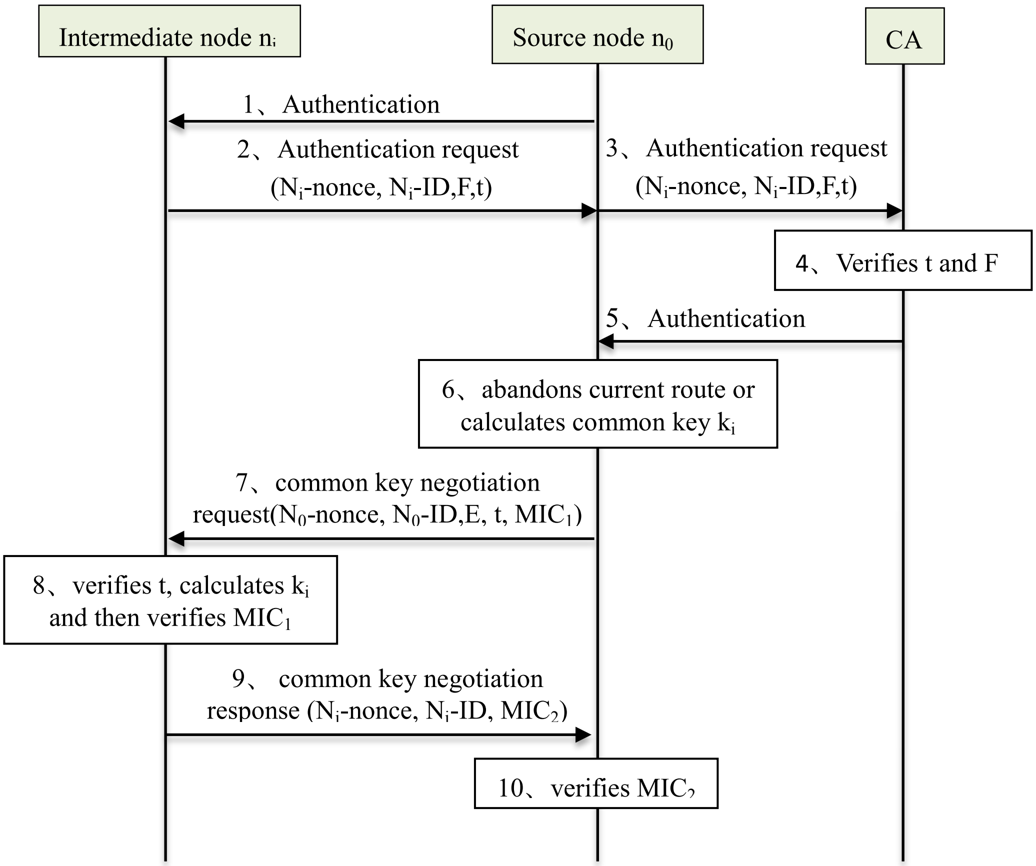

Intermediate node $n_i$
Source node $n_0$
CA
1、Authentication
2、Authentication request ($N_i$-nonce, $N_i$-ID,F,t)
3、Authentication request ($N_i$-nonce, $N_i$-ID,F,t)
4、Verifies t and F
5、Authentication
6、abandons current route or calculates common key $k_i$
7、common key negotiation request($N_0$-nonce, $N_0$-ID,E, t, $MIC_1$)
8、verifies t, calculates $k_i$ and then verifies $MIC_1$
9、 common key negotiation response ($N_i$-nonce, $N_i$-ID, $MIC_2$)
10、verifies $MIC_2$

**Figure 4. Detailed Description of Stage 1 and Stage 2**

Step 1: Node $n_0$ sends a packet to Node $n_i$ firstly to inform it that $n_0$ intend to transmit information via $n_i$, meanwhile activates authentication process.

Step 2: The authentication to $n_i$ is started from $n_i$, The first authentication message {Ni-nonce, Ni-ID,F,t} is sent to the source node $n_0$ from $n_i$, among which t is a counter and its initial value is set as 1. The $n_i$ increases the counter by one once sending such a message. $N_i$-nonce is a random value generated by $n_i$. $N_i$-ID is the $n_i$ identity, it is generated for each node by CA during $n_i$ accessing CA. In which,

$$F=\text{Encrypt}_{kpri}(f(N_i\text{-nonce}||N_i\text{-ID}||t))$$

Where f() is a hash function, || denotes the concatenation and $k_{pri}$ is the $n_i$'s private key. $\text{Encrypt}_{pri}()$ means that $n_i$ encrypts $f(N_i\text{-nonce}||N_i\text{-ID}||t)$ with private $k_{pri}$.

Step 3: Source node $n_0$ receives the message {Ni-nonce, Ni-ID,F,t} from $n_i$ and transmits it to the CA.

Step 4: Upon receiving the authentication message,CA gets its $N_i$-ID and t, and then compares t with the value which has been preserved in CA previously. Because counter t is also set in the CA for each node and its initial value is also set as 1. If the received t value is less than the t value in CA, the authentication of the $n_i$ fails and the current t value of the CA will not changed; otherwise, the CA will further decrypt F with $n_i$'s public key. If correct, the authentication of the $n_i$ by the CA succeeds, and the CA increases the received t value by one and sets it as its current t value.

Step 5:The CA replies to the $n_0$ with the authentication response message.

Step 6: Source node $n_0$ decides to the further action according to the result of the $n_i$'s authentication by the CA. If authentication is failing, $n_0$ will abandon this routing path and then seek another route. Otherwise, $n_0$ will fulfill two tasks. Firstly, $n_0$ will record the $n_i$'s $N_i$-ID and its corresponding value of t for authentication in the next stage 3. Secondly, $n_0$ will calculate common key $k_i$ used for subsequent communication between $n_i$ and $n_0$.Common key $k_i$ is calculated by equation as follows.

$$k_i=h(p_{kni},\text{"common\_key"}||N_0\text{-nonce}||N_0\text{-ID}||N_i\text{-nonce}||N_i\text{-ID}||t)$$

In the above equation, h() is a hash function, $p_{kni}$ is $n_i$'s public key, "common_key" is a constant string, $N_0$-nonce is a random value generated by $n_0$ and $N_0$-ID is the $n_0$ identity.

Step 7: Subsequently $n_0$ will send key negotiation message{$N_0$-nonce, $N_0$-ID,E,t,$MIC_1$},in which

$$E=f(p_{kni}, N_0\text{-nonce} ||N_0\text{-ID} ||t)$$

Where $MIC_1$ is the message authentication code computed on this message by the $n_0$ using the $k_i$,and t is the current t value of $n_i$ in the $n_0$.

Step 8: When $n_i$ receiving the message from $n_0$, $n_i$ will compare the received t value with t value in itself, and if equal or more than current t value, $n_i$ will validate E further by its private key $k_{pri}$.If correct, the authentication of the $n_0$ will pass. Thereafter, $n_i$ will compute the common key $k_i$ using the same method as that of the $n_0$. On $k_i$ is figured out, $n_i$ will verify the $MIC_1$ taking use of the $k_i$. If valid, $n_i$ will install the $k_i$ to communicate with $n_0$ in the subsequent procedure.

Step 9: Intermediate node $n_i$ sends the common key negotiation response message{$N_i$-nonce, $N_i$-ID, $MIC_2$}to source node $n_0$, where $MIC_2$ is the message authentication code computed on this message by $n_i$ using the common key $k_i$.

Step 10: $N_0$ immediately verifies the $MIC_2$ after receiving the response message form the $n_i$. If correct, it means $n_i$ generates the same common key $k_i$. So far, the networks side completes the authentication of the $n_i$, and the $n_i$ and $n_0$ both install the common key $k_i$.

The description of stage 3 is as follows.

$$MIC_i=encrypt_{ki}(f(r_i||msg))$$
$$E_i=encrypt(r_i)$$

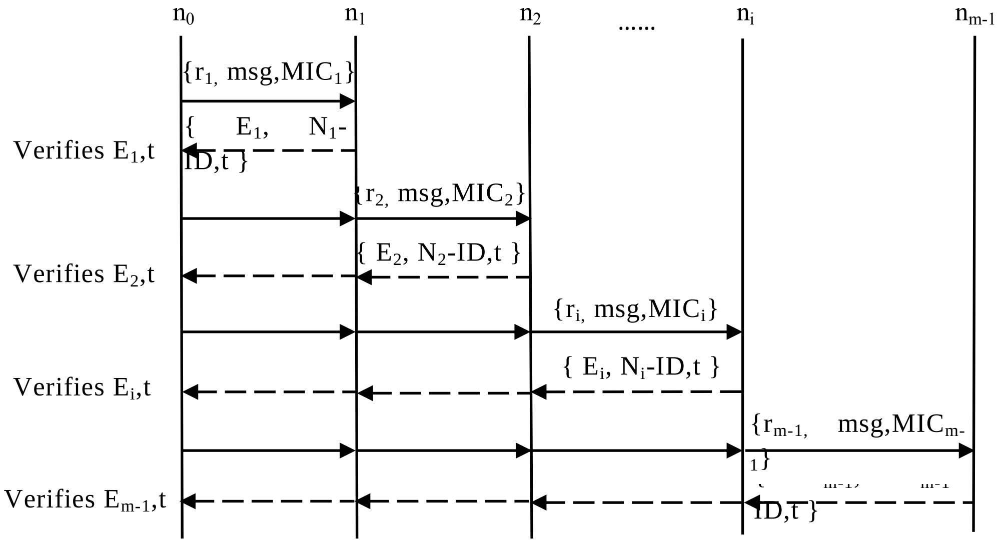


**Figure 5. Detailed Description of Stage 3**

As shown in Figure 5, source node $n_0$ send the first route authentication message$\{r_1,msg,MIC_1\}$ to $n_1$,in which $r_1$ is a random value generated by $n_0$ and $MIC_1$ is message authentication code. Random value $r_1$ acts as a challenge to $n_1$. Upon $n_1$ receiving the first message, it will encrypts challenge $r_1$ with the common key $k_1$ between $n_0$. At the same time, $n_1$ will verify the $MIC_1$ taking use of the $k_1$. If valid, the authentication reply message $\{E_1, N_1\text{-ID}, t\}$ is transmited to the $n_0$.

Where $E_1=\text{encrypt}_{k1}(r_1)$

$N_1$-ID is $n_1$'s identity and t is the counter of $n_1$, both of which has recorded in the $n_0$ during stage 2.

When $n_0$ receiving the response message from $n_1$, it will compare the $N_1$-ID and t with the value of them recorded in itself. If one of their authentication fails, $n_0$ will discard this message and $n_1$ is suspected as a delicious node. Of course, the current routing path will be abandon. In contrast, if both of them is authenticated successfully, subsequently, $n_0$ will decrypt $E_1$ and verify $r_1$.If the received $r_1$ is unequal with the sent value of it, the current route is abandoned. Only if the authentication of $r_1$ is also successful, the $n_1$ is passed and subsequently the authentication of the next node during the routing path is launched by $n_0$ using the same method as that of $n_1$.

The authentication process above is repeated during the other nodes in the current route until one of them is failing. If the authentication of all nodes is successful, the current route is authenticated successful. The communication between $n_0$ and $n_{m-1}$ is started.

### 4.3. Some Considerations of the Scheme

When the scheme is designed, some related problems are considered including several negative affection brought by the scheme, such as delay. Some of them are analyzed as follows.

1. The proposed scheme involved three stages covers all the authentication procedure, the additional overheads of authentication is still tolerable, the simulation result is shown in section below. Because the accessing authentication and the negotiation of common key $k_i$ in stage 1 and stage 2 is greatly simplified compared with traditional authentication based on 802.11i, though the authentication of route in stage 3 is added. All the overheads through the whole authentication is less than watch dog in [8] and the scheme proposed in [15].

2. In stage 2, the source node $n_0$ and intermediate node $n_i$ respectively send their random value and ID to the opposite side for calculating the common key $k_i$. The key $k_i$ is not transmitted between $n_0$ and $n_i$, thereby the $k_i$ is avoided to be intercepted by the third side.

3. In proposed scheme, the t is added in three stages. This measure is used to resist replay attacks combined with random value nonce on the one hand. On the other hand, it is used to verify the intermediate node $n_i$'s identity combined with $n_i$'s ID.

4. In stage 3, $n_0$ verifies $n_i$'s identity according to the related value in received message. We only consider about the condition in which the message is modified by the malicious node. The packets are also possibly discarded in the black hole attack. To manage this attack, the timer is set in the $n_0$. Once $n_0$ hasn't received the replay message in certain time, $n_i$ is suspected as malicious and the current route is abandoned.

5. In [15], the source node $n_0$ only sends one message to the other node in the routing path. In contrast, $n_0$ sends one message to each other node. In the condition of few malicious node, the former is better. But if the malicious nodes are more, the latter is

preferable. Because the authentication procedure to $n_i$ will be terminated when one node's authentication is failing. The authentication of rest of nodes in the route is needless.

## 5. Simulation and Analysis

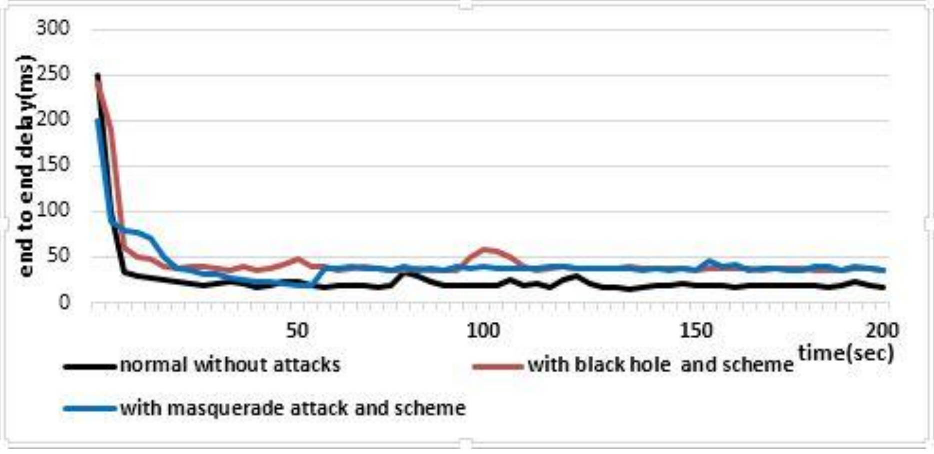
The simulator which we conducted our solution making use of is the network simulator (ns-2.35) [16] . In the hypothetical network, 50 wireless mobile nodes move randomly in a square area with the size of 1000 meter. Nodes' movement and position according to the random waypoint model. The related simulation parameters shown in Table 1. Some simulation parameters described below.

**Table 1. Parameters in Simulation**

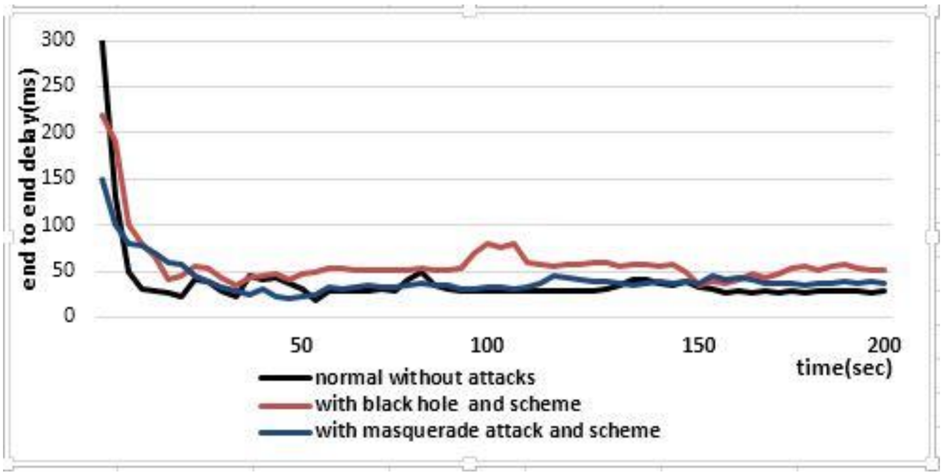
| Parameters | Values |
|---|---|
| Simulation area | 1000*1000 |
| mobility model | random way point |
| Link Layer type | LL |
| Protocols studied | AODV/DSR |
| Simulation time | 100 sec |
| Maximum speed | 20m/s |
| Maximum Pause time | 5 sec |
| Traffic type | CBR(UDP) |
| CBR rate | 50 Kbps |
| Number of nodes | 30 |
| Number of Malicious Nodes | 2 |
| Hash function | SHA-1 |

### 5.1. End-to-End Delay

End-to-end delay represents the time required to move the packet from the source node to the destination node.



(a) AODV-based Network



(b) DSR-based Network

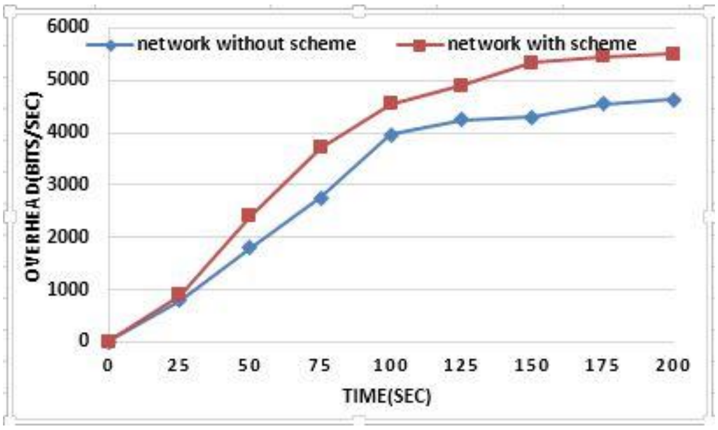
**Figure 6. End to End Delay**

End to end delay in both AODV-based network (Figure 6(a)) and DSR-based network (Figure 6(b)) is illustrated respectively. At the beginning of simulation, the delay is significant in three cases: normal network without attacks, network with black hole and scheme and network with masquerade attack and scheme. The big delay is caused by $n_i$ accessing network authentication, negotiating the common key $k_i$ and the source node $n_0$ checking all the received acknowledgments from $n_i$ and discovering a new route.

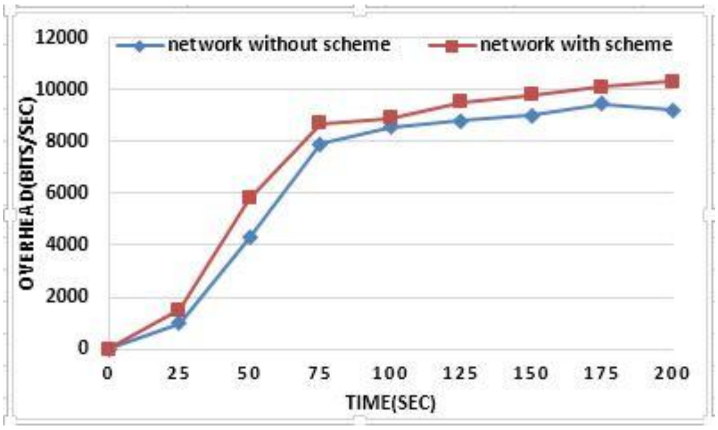
We note that the delay, at the start, in the both cases under two type of attacks is smaller than that in normal network, because the 802.11i is adopted used for authentication in normal one. The results shown that the proposed scheme taken smaller time in node accessing network than 802.11i.But the delay is reducing more slowly in normal network of proposed scheme than that. The reason is that proposed scheme needs to take some time in authenticating all nodes in route. The simulation shown that the graphs eventually become almost identical and converge to the normal state without attack.

### 5.2. Additional Communication Overheads

Because authentication, our approach brings an additional communication overheads. The main overheads we measure is in stage 3. The overheads results on the information relating authentication which involves the random value $r_i$ and message authentication code $MIC_i$ accompanying the message msg sent by $n_0$. Additionally, the authentication replay message is another part of overheads.



(a) AODV-based Network



(b) DSR-based Network

**Figure 7. Additional Communication Overheads**

Figure 7. Shown the additional overheads in AODV-based network and DSR-based network respectively. We measure the overheads in network with proposed scheme compared with the value without scheme. The simulation results indicate that proposed scheme increases the overheads by 10 percentage around. The selective measures to reduce the overheads is that the source node n0 can select randomly some intermediate nodes instead of all of them, and asks them to send the response messages. The authentication response information involving in the data packets can reduces the overheads further.

## 6. Conclusion

Ad Hoc network is vulnerable to some typical attacks for its own characteristics. The authentication scheme proposed in this paper composed by three stages. The scheme consisted of stage 1 and stage 2 is a improvement based on 802.11i for $n_i$ to access the network and generating the common key $k_i$. The stage 3 mainly authenticates the whole routing path. The simulation results indate that the delivery ratio and end to end delay of proposed solution is similar to the network without attacks. It signifies that the solution is efficient. Meanwhile, the overhead introduced by authentication is tolerable.

## References

[1] X. Wang, T. liang Lin and J. Wong, "Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network", Technical Report, Computer Science, Iowa State University, **(2005)**.

[2] H. Nakayama, Y. Nemoto and N. Kato, "A Survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE Wireless Communications, **(2007)** October.

[3] J. Luo, M. Fan and D. Ye, "Black Hole Attack Prevention Based on Authentication Mechanism", IEEE, **(2008)**, pp. 173-177.

[4] C. E. Perkins and E. M. Belding-Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing", http://www.ietf.org,RFC3561, **(2003)** July.

[5] L. Haiyan and S. Zhanlei, "Comparing the performance of the Ad Hoc network under attacks on different routing protocol", **(2015)** June, pp. 195-208.

[6] D. B. Johnson, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", http://www.ietf.org, RFC4728, **(2007)** February.

[7] Ms. N. Sha rma and Mr. A. Sharma, "The Black-hole node attack in MANET", 2012 Second International Conference on Advanced Computing & Communication Technologies, pp. 546-548.

[8] S. Marti, T. J. Giuli, L. Kevin and B. Mary, "Mitigating routing misbehavior in mobile ad hoc networks", in: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), **(2000)**, pp. 255–265.

[9] D. Djenouri and N. Badache, "Struggling against selfishness and black hole attacks in manets", Wireless Commun. Mobile Comput., vol. 6, **(2008)**, pp. 689–704.

[10] Y. Yu, G. Lei, W. Xingwei and L. Cuixiang, "Routing security scheme based on reputation evaluation in hierarchical ad hoc networks", Compute Network, vol. 54, **(2010)**, pp. 1460–9.

[11] Karlof C. and Wagner D., "Secure routing in wireless sensor networks: attacks and countermeasures", **(2003)** September, pp. 293–315.

[12] D. Djenouri and N. Badache, "On eliminating packet droppers in MANET: a modular solution, Ad Hoc Networks", vol. 7, no. 6, **(2009)**, pp. 1243–1258.

[13] S. D. Manikantan, C. Yu and A. Tricha, "Channel-aware detection of gray hole attacks in wireless mesh networks", IEEE global telecommunications conference, **(2009)** December, pp. 1–6.

[14] C. Hongsong, J. Zhenzhou and H. Mingzeng, "A novel security agent scheme for AODV routing protocol based on thread state transition", Asian J. Informat. Technol., vol. 5, no. 1, **(2006)**, pp. 54–60.

[15] A. Baadache and A. Belmehdi, "Struggling against simple and cooperative black hole attacks in multi hop wireless ad hoc networks", Computer-Networks, **(2014)**, pp. 173-184.

[16] M. Mohanapriya and I. Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET", Computers and Electrical Engineering, vol. 40, **(2014)**, pp. 530–538.

[17] N. Shanmugam Bhalaji and A. Anna Univ., Coimbatore, "Association between nodes to combat blackhole attack in DSR based MANET", Wireless and Optical Communications Networks, **(2009)**, pp. 103–115.

## Authors

**Haiyan Liu,** received her BS in Physical Education from Henan Normal University, Xinxiang, China, in 2000.She got her MS in Subject Teaching Theory from Henan Normal University, Xinxiang, China, in 2003. She is a Lecturer in the Engineer Training Center at Zhengzhou University of Light Industry. Her research interests include computer network and network security.

**Kongjun Bao,** received his BS in Electrical Technology from Zhengzhou University of Light Industry, Zhengzhou, China, in 1987. He got his MS in Computer Application from Huazhong University of Science and Technology, Wuhan, China, in 2003. He is an Associate Professor in Engineer Training Center at Zhengzhou University of Light Industry. His research interests include network database and multimedia.