International Journal of Networked and Distributed Computing, Vol. 2, No. 2 (April 2014), 100-107

Using Cryptographic Technique for Securing Route Discovery and Data Transmission from BlackHole Attack on AODV-based MANET

Seryvuth Tan
Department of Computer Science, Konkuk University
Seoul, Republic of Korea
E-mail: seryvuth-tan@nida.gov.kh

Phearin Sok
Department of Computer Science, Konkuk University
Seoul, Republic of Korea
E-mail: phearin.sok@gmail.com

Keecheon Kim*
Department of Computer Science, Konkuk University
Seoul, Republic of Korea
E-mail: kckim@konkuk.ac.kr
www.konkuk.ac.kr

Abstract

MANET is a dynamic wireless network without any infrastructures. The network is weak and vulnerable to many types of attacks including BlackHole attack. BlackHole node advertises itself as having freshest or shortest path to a specific node to absorb packets. The effect of BlackHole attack on AODV will be addressed in this paper by using cryptography technique for securing route discovery and data transmission. Simulation results using NS2 depict the improvement of packet delivery ratio and network throughput in the presence of BlackHole nodes.

Keywords: MANET; AODV; BlackHole Attack; Cryptographic Technique.

1. Introduction

A Mobile Ad-hoc Network (MANET) is a self-organized wireless network of mobile nodes without any fixed infrastructure. Nodes roam through the network, causing its topology to change rapidly and unpredictably over time. New nodes can join the network, whereas at the same time other nodes leave it or just fail to connect (temporarily) because they move to a region that is not in the cover range of the network. Nodes are typically wireless devices such as PDAs, laptops or cellular phones. From the very beginning, the use of MANETs has been appealing for both military and civilian applications, especially in the last decade because of development of wireless LAN technology.

Due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks[1]. These include passive eavesdropping, active interfering, impersonating, and denial-of-service. BlackHole attack is one of many possible attacks in AODV-based MANETs. In this attack, a malicious node sends a

Published by Atlantis Press

forged route reply (RREP) packet to source node that initiates the route discovery in order to pretend to be the destination node. The standard of AODV protocol, the source node compares the destination sequence number contained in RREP packets when a source node received multiple RREP, it judges the greatest one as the route contained in that RREP packet. In case the sequence numbers are equal, it selects the route with the smallest hop count. As the result, the data transmission will flow toward the malicious node by source node and it will be dropped.

The ultimate goal of the security solutions for AODV protocol is to provide security services, such as authentication, confidentiality, integrity, anonymity and availability to mobile users. In order to achieve these goals, we will concentrate in addressing a security concern related to routing discovery and data exchange. A modified protocol will be proposed that accumulate the routing, authentication, generation and secure exchange of public key, private key and session key. They would be facilitating the users to establish parameters during the route discovery session and the parameters would subsequently be used to ensure confidentiality and integrity of data exchange.

The remaining of the paper is organized as follows. Section II introduces AODV routing protocol. BlackHole attack is described in section III and section IV presents related works. Next, in section V we propose our mechanism and section VI is the simulation and evaluation. Finally, the conclusion is depicted in section VII.

2. AODV Routing Protocol

Ah-hoc On-demand Distance Vector (AODV) is used to find a route between source and destination as needed and there are three significant types of messages used in this routing protocol such as route request (RREQ), route reply (RREP) and route error (RRER).

The information fields of these messages, such as source IP address, destination IP address, source and destination sequence number, hop count and etc. are presented in detail in Ref. 2. Each node uses this information which contains in a routing table for routing to a specific destination. When a source node wants to communicate with a destination and there is no any route between them in the routing table, at first step the source node broadcasts RREQ as shown in the Fig1. The RREQ is received by intermediate nodes that they

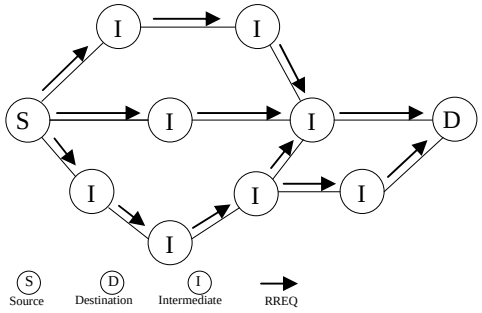

Fig. 1. Broadcasting RREQ message

are in the transmission range of the sender. These nodes broadcast and forward this RREQ packet until it is received by destination or an intermediate node that has fresh enough route to the destination.

Then the destination sends RREP unicast toward the source as shown in the Fig. 2. Hence, a route among the source and destination is established. A fresh enough route is a valid route entry that its destination sequence number is at least as great as a destination sequence number in RREQ packet. The source sequence number is used to determine freshness about route to the source. In addition, the destination sequence number is used to determine freshness of a route to the destination. When

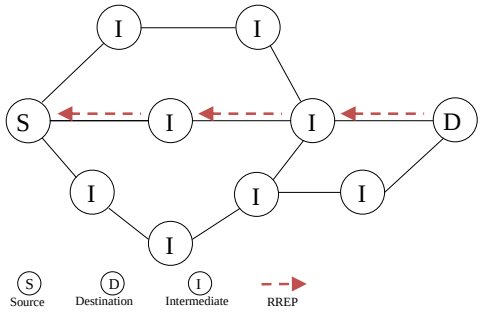

Fig. 2. Unicasting RREP message

intermediate nodes receive RREP with consideration of destination sequence number and hop count, it creates or updates a forward route entry in its routing table for that destination.

In Route Maintenance procedure, nodes keep an entry for each active route in their routing table and periodically broadcast Hello message to its neighbors in order to detect a possible link failure. If a node detects a link failure, it knows that all active routes via this link fail. So a Route Error message (RERR) is sent to

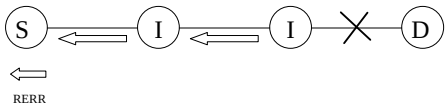

Fig. 3. Transferring RERR message

announce all relative source nodes as shown in the Fig.3. The source nodes then will decide whether to refresh the route or not.

3. BlackHole Attack

Routing protocols are exposed to a variety of attacks. BlackHole attack[3] is one kind of Denial Of Service (DoS) attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. The malicious node responds immediately to the source node without following the routing protocol rules. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by

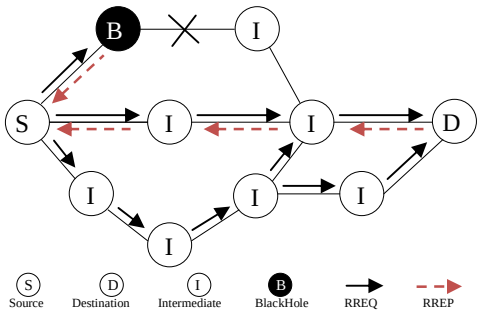

Fig. 4. Illustration of BlackHole Attack

assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires.

As an example, consider the following scenario in Fig. 4. We illustrate a typical scenario of the protocol packet exchanges, generation and traversal of RREQ and RREP control messages. The node S is assumed to be the source node or originating node desiring to communicate with node D (destination node). Thus, as the earlier explanation, node S generates the RREQ control message and broadcasts it. The broadcasted RREQ control message is expected to be received by neighbor nodes. Assuming that the node B is a malicious node (BlackHole node) in the network, and the node I (Intermediate node) has a route to node D in its route table. The node I will forward RREQ until to reach the destination and update its routing table with the accumulated hop count and the destination sequence number.

However, since the destination sequence number is high, the route from node B will be considered to be fresher and hence node S (source node) will start sending data packets to node B that is malicious node. At the same time RREQ control message from node I will eventually reach node D (destination node), which will generate RREP control message and route it back. However, since the node S has a RREP control message with higher destination sequence number to that route, node S will ignore other RREP control messages. If any link is disconnected during the transfer of packets then RERR control message is generated.

Therefore, in order to fake AODV using BlackHole attacks, the attacker uses two methods:

- Send RREP packet towards the source node with highest enough sequence number.
- Send RREP packet to source node with small enough hop count number

In most cases, the BlackHole attack gains the route if the routing protocol does not protect itself. BlackHole attack does not follow the routing protocol rules by not spending a long time to reply. Hence, BlackHole attack produces quicker reply of RREP than the real destination node or other node in the network by coping source and destination address from RREQ packet, decreasing hop count and increasing highest sequence number.

4. Related Works

The research in MANETs is a broad topic covering routing and security. Moreover, there are many research papers about the BlackHole attack defense strategies in MANETs. This section only gives a brief discussion of some researches that closely relate to the idea of this paper:

Lu et al[4] proposed a BlackHole detection scheme (so called SAODV) for MANETs that addressed some security weaknesses of AODV and withstand the BlackHole attack. An enhanced version of this SAODV protocol was provided by Deswal and Singh[5], where a password security was used for each routing node and routing tables were updated in a timeliness fashion.

Secure Routing with AODV (SRAODV), a series of security mechanism, including Key Exchange, Secure Routing, Data Protection, are proposed by A. Pirzada and C. McDonald[6]. Considering about secure routing mechanism, the author recommended peer-to-peer symmetric encryption to all routing information in RREQ, RREP and RRER, using a group session key negotiated by neighbor nodes. However, this design requires each node to maintain a table along with associated group members and session keys. It would become less efficient as the number of nodes in ad hoc network increase. And moreover, a compromised node could still juggle hop_count or destination sequence number to interrupt the normal routing procedure.

Authentication Routing for Ad-hoc Network (ARAN)[7] secure routing protocol proposed in recent and uses cryptographic certificates to prevent and detect most of the security attacks that most of the ad hoc routing protocols face. This protocol introduces authentication, message integrity and non-repudiation as part of a minimal security policy for the ad hoc environment.

ARAN consists of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication. Thus, the routing messages are authenticated end-to-end and only authorized nodes participate at each hop between source and destination.

The most of research papers above are discussed about secure routing protocol on MANET to avoid some attacks based on the AODV protocol and other protocols. However, our solution in this paper provides the security on routing packets by using the cryptographic technique in one step for preventing BlackHole attacks on AODV-based MANET.

5. Our Proposed Mechanism

AODV protocol would be the basis of our propose work. Route Request (RREQ), Route Reply (RREP) and Route Error (RRER) are the message types defined by AODV[2].

In addition to our previous work[8] of securing route discovery in ADOV protocol, we propose a new mechanism for two ways of securing not only route discovery, but also data transmission by using a cryptography technique.

This protocol is a new protocol based on the traditional AODV protocol. The designed protocol encompasses the routing mechanism and exchange of security parameters in a single step. This would be considered as a major change from the current security techniques used in AODV and conventional security protocols affiliated with the network and transport layer.

5.1. *Assumption*

Certificates can be issued to all participating nodes in relation to their MAC address or IP address, personal credentials or on any agreed pattern. The mechanism of issuing certificates by CA is considered out of the scope of this paper. It is assumed that trust relationship exists only between a source and destination node. Intermediate nodes participating in routing are out of trust relationship.

5.2. *Basic Ideas*

Our proposed work includes the following ideas:

- The Certification Authority (CA) will be used to request destination public key by only source node.
- The concept of asymmetric cryptography (public key and private key cryptography) will be used for the secure route discovery and exchange of session key.
- Use of symmetric cryptographic techniques[9] such as Advance Encryption Standard (AES)[10] for data encryption

Following symbols will be used in the proposed options, source node (S), destination node (D), BlackHole node (B), Intermediate node (I), Source IP address (S_{IP}), Destination IP address (D_{IP}), Public key of x (K_{BX}), Private key of x (K_{AX}), where x is either source or destination. E_K encryption using key K, D_K decryption using key K, Session key (K_S), Routing Request (RREQ) and Routing Reply (RREP).

5.3. *Analysis*

Fig. 5 illustrates the secure route discovery and data transmission process of MANET on AODV protocol.

As we mention above, the trust relationship already existed between source node and destination node. Therefore, destination node's public key is known by CA. In our mechanism, we assume that source node already got the destination public key (K_{BD}) from CA.

The originating node or source node generates a Route Request (RREQ), and attaches its public key (K_{BS}) decrypted by destination public key (K_{BD}) from

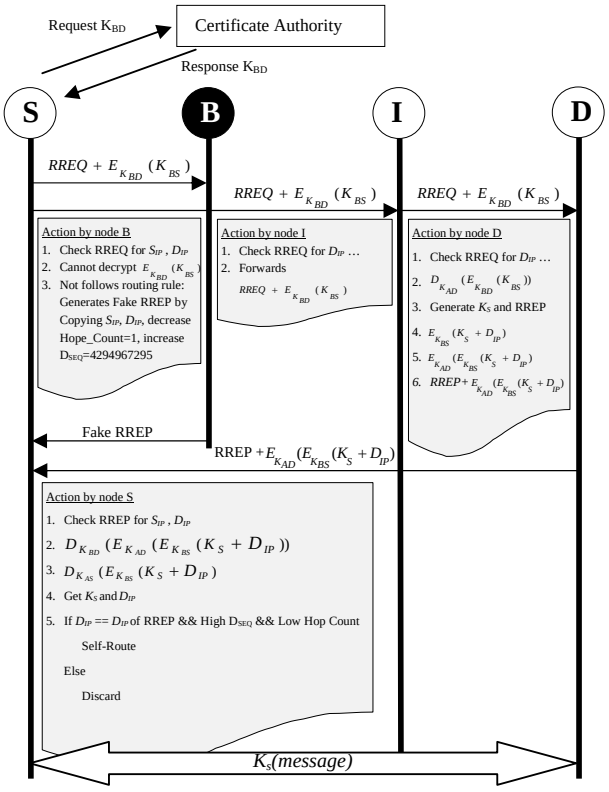

Fig. 5. Algorithm to secure routing protocol and data transmission

CA.

$$RREQ + E_{K_{BD}}(K_{BS}) \quad (1)$$

This packet is broadcasted by source node to all neighbor nodes or intermediate nodes for route discovery of destination. On the network, both intermediate nodes and BlackHole nodes receive the same this packet.

5.3.1 The process of intermediate nodes:

On reception of the $RREQ + E_{K_{BD}}(K_{BS})$ packet, the intermediate node initials checking destination IP address in RREQ by verifying this IP address in its routing table. The $RREQ + E_{K_{BD}}(K_{BS})$ packet will be forwarded with increasing hop count plus one in RREQ if this node is not a destination. Typically, the $RREQ + E_{K_{BD}}(K_{BS})$ packet will be forwarded by the intermediate nodes until it reaches the destination without decrypts source public key $E_{K_{BD}}(K_{BS})$.

5.3.2 The process of BlackHole nodes:

The BlackHole attack manner does not follow the routing rule and spends a lot of time to reply the Route Reply (RREP) packet. When it receives $RREQ + E_{K_{BD}}(K_{BS})$ packet, it suddenly generates RREP to the source node by copying destination and source IP address from RREQ, setting hop count to lowest as 1 and increasing destination sequence number to maximum of sequence number as 4294967295 [2]. The BlackHole attack cannot get the source public key because it doesn't have the destination private key (K_{AD}) to decrypt the destination public key (K_{BD}). The fake RREP packet generated by BlackHole node suddenly is replied to the source node.

5.3.3 The process of destination nodes:

After checking its IP address in RREQ, the destination node gets the source public key (K_{BS}) by using its private key (K_{AD}) to decrypt $E_{K_{BD}}(K_{BS})$.

$$D_{K_{AD}}(E_{K_{BD}}(K_{BS})) \quad (2)$$

A session key (K_S) and a Route Reply (RREP) are generated by destination node and destination node uses the source public key (K_{BS}) to encrypt the session key (K_S) and destination IP address (D_{IP}).

$$E_{K_{BS}}(K_S + D_{IP}) \quad (3)$$

The destination node then encrypts $E_{K_{BS}}(K_S + D_{IP})$ with its private key (K_{AD}) for authentication.

$$E_{K_{AD}}(E_{K_{BS}}(K_S + D_{IP})) \quad (4)$$

Finally, the Route Reply (RREP) attached with $E_{K_{AD}}(E_{K_{BS}}(K_S + D_{IP}))$ is unicasted toward to the source node along the route by destination node.

$$RREP + E_{K_{AD}}(E_{K_{BS}}(K_S + D_{IP})) \quad (5)$$

5.3.4 The process of source node when receives packet:

The originating node or source node receives two packets from its neighbors. The source node will consider whether which one is a secure packet by following using the algorithms:

(a) The packet from destination node

- The source node obtains the source and destination IP address from Route Reply (RREP)
- The source node confirms the authenticity of destination node by using the destination public key (K_{BD}) to decrypt destination private key (K_{AD})

$$D_{K_{BD}}(E_{K_{AD}}(E_{K_{BS}}(K_S + D_{IP})) \quad (6)$$

- The source node decrypts $E_{K_{BS}}(K_S + D_{IP})$ obtained from the previous algorithm $D_{K_{BD}}(E_{K_{AD}}(E_{K_{BS}}(K_S + D_{IP}))$ by using the source private key (K_{AS}) for session key (K_S) and destination IP address (D_{IP}).

$$D_{K_{AS}}(E_{K_{BS}}(K_S + D_{IP}) \quad (7)$$

(b) The packet from BlackHole attack node

- The source node obtains the source and destination IP address from Route Reply (RREP)
- No encryption packet

The source node will consider the self-route using the following criteria :

- Verify whether the destination IP addresses both from RREP packet and its encrypted attachment $E_{K_{AD}}(E_{K_{BS}}(K_S + D_{IP})$ are equal.
- High destination sequence number (D_{SEQ})
- Low hop count

Otherwise, the other received packet will be discarded by source node. The source node uses the session key (K_S) generated by destination node for secure data transmission between the source node and destination node.

6. Simulation and Evaluation

We use a standard simulation NS2 for simulation[11]. Network simulation (NS2) is an event driven simulation tool and designed specifically to study the dynamic nature of wireless communication networks. To evaluate it with standard AODV protocol in the presence of the BlackHole attack on the network. We define 50 nodes for our simulation. One of those nodes is simulated as BlackHole node.

Pause time is varied from 0 to 80 sec. Each node in MANET is assigned an initial position within the simulation dimensions (1000*1000) meters and joins the network at a random time. The packets are generated using CBR with packet size 64 bytes for all mobile nodes. Random Waypoint Model (RWP) is used as the mobility model of each node. In random-based mobility models, the mobile nodes move randomly and freely without restrictions. To be more specific, the destination, speed and direction are all chosen randomly and independently of other nodes. The simulation parameters are captured in Table 1.

Table 1. Simulation Parameters.

Parameter	Setting
Simulation area size	1000m * 1000m
Number of nodes	50
MAC protocol	IEEE 802.11
Radio range of a node	250m
Traffic type	CBR
Traffic data rate	100 Kbytes
Network layer protocol	AODV
Simulation time	10 minutes
Mobility model	Random way point
Speed	Random (0-80 m/s)
Packet size	64 bytes
Pause time	Random (0-80 s)

The proposed modifications on the existing AODV protocol have been a successful integration of routing and exchange of data security key which include:

- Source public and private key by source node.
- Destination public and private key by destination node.
- Session key by destination node

The added parameters in the RREQ message include:

- Source public key is encrypted by destination public key

On the reception of RREQ, the destination responds with RREP having additional parameters including:

- Session key and destination IP address are encrypted by source public key and continue to encrypt by destination private key

The session key received by the source node uses symmetric encryption technique in AES[10]. It is used for encryption data message from source to destination. Thus, routing and exchange of session key have been ensured in a single step.

We consider node mobility scenarios to analyze the simulation results based on the performance metrics as below:

- Packet delivery ratio: This represents the ratio between the number of packets originated by the "application layer" CBR sources and the number of packets received by the CBR sink at the final destination.
- Network Throughput: This represents the average rate of successful message delivery over a communication channel and can be measured as bits per second (bps).

The first performance metric we used in the analysis of our mechanism is the packet delivery ratio. Fig. 6 depicts the effect of the packet delivery ratio on the node mobility in the presence of the BlackHole attack in the network, where node mobility (mps) is the rate at which the nodes are moving in the network. It can be observed that AODV suffers heavy loss in packets in the presence of a BlackHole node, by dropping from above 90% to below 70%. However, our protocol scheme gives a higher (no less than 85%) and consistent packet delivery ratio even in the presence of a BlackHole node.

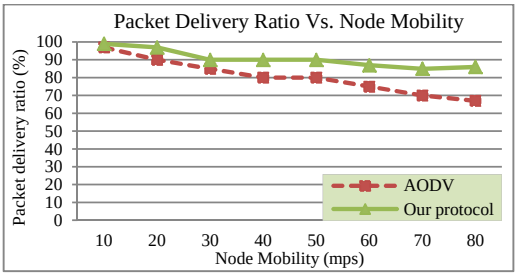

Fig. 6. Packet Delivery Ratio Vs. Node Mobility

Fig. 7 depicts the effect of the packet delivery ratio on the pause time. It can be observed that the packet delivery ratio of the AODV scheme drops dramatically to about 70% and continues to drop as the pause time is increased. In contrast, our protocol scheme, producing in-between 90% of delivery ratio, is able to achieve better results in the presence of the BlackHole node compared to the standard AODV. This may be justified by the fact that the standard AODV does not have any built-in security mechanism.

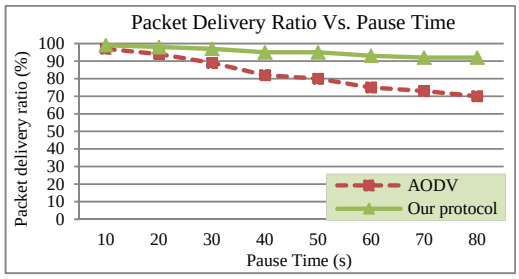

Fig. 7. Packet Delivery Ratio Vs. Pause Time

The second performance metric we used in the analysis of our mechanism is the network throughput. The effect of the network throughput on the node mobility and pause time are depicted on Fig. 8 and Fig. 9, respectively. It can be observed that the standard AODV protocol under BlackHole attack has the lowest throughput when compared to that of our protocol. Both of the Fig. 8 and Fig. 9 show that the traditional AODV with the BlackHole node presence produces maximum network throughput of 470 and 440, respectively. Meanwhile, our proposed protocol develops maximum throughput of 500 and 510 for Fig. 8 and Fig. 9, respectively.

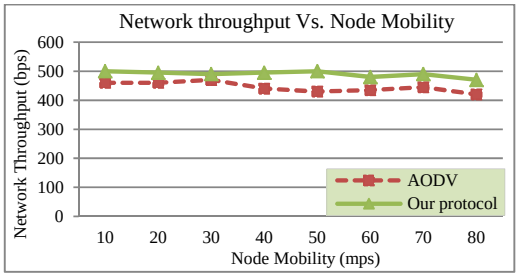

Fig. 8. Network Throughput Vs. Node Mobility

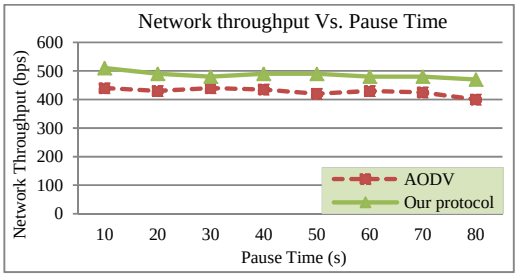

Fig. 9. Network Throughput Vs. Pause Time

7. Conclusion

Security issues have been overlooked while designing routing protocols for ad-hoc networks. According to standard AODV protocol, it is susceptible to many malicious attacks including BlackHole Attacks. The proposed protocol, Secure Route Discovery and Data Transmission from BlackHole Attacks on AODV-based Mobile Ad-hoc Networks is the mechanism that uses the cryptographic technique (using public, private and session key) for securing route discovery and data transmission. In our proposed mechanism provides high ability to prevent BlackHole attack in the network thus the packet loss will be reduced. In future work, we will improve the credibility of AODV on route discovery and data transmission.

Acknowledgements

This research was supported by the IT R&D program of MKE/KEIT [10041910, Development of global cloud delivery platform that can reduce video traffic up to 50%].

References

1. R. H. Khokhar, A. N. Ngadi, A. Mandala, *A review of current routing attacks in mobile ad hoc networks*, Intl. Journal of Computer Science and Security, vol. 2, Issue-3, (2008), pp. 18-29
2. C. E. Perkins, E. M. B. Royer and S. R. Das, *Ad-hoc On-Demand Distance Vector (AODV) Routing*, Mobile Ad-hoc Networking Working Group, Internet Draft, draft-ietf-manetaodv- 00.txt, (Feb, 2003).
3. M. Al-Shurman, S-M. Yoo, and S. Park, *BlackHole Attack in Mobile Ad Hoc Networks*, ACM Southeast Regional Conf, (2004).
4. S. Lu, L. Li, K-Y Lam, L. Jia, *SAODV: A MANET Routing Protocol that can Withstand BlackHole Attack*, Proc. of Intl. Conference on Computational Intelligence and Security (CIS '09), Dec. 11-14, (Beijing, China, 2009), pp. 421-425.
5. S. Deswal and S. Singh, *Implementation of Routing Security Aspects in AODV*, Intl. Journal of Computer Theory and Engineering, Vol. 2, No. 1, (Feb, 2010).
6. A. Pirzada, C. McDonald, *Secure routing with the AODV protocol*, Proc. The Asia-Pacific Conference on Communications, (2005), 57-61.
7. B. Dahill, B.N. Levine, E. Royer, and C. Shields, *ARAN: A secure routing protocol for ad hoc networks*, UMass Tech Report 02-21, (2002).
8. S. Tan, M. Choi, K. Kim, *The New Mechanism to Detect and Prevent BlackHole Attacks on AODV-based MANET*, Vol. 684, (April 2013), pp. 547-550.
9. B. Schneier, *Applied cryptography*. J. Wiley and sons inc, (1996).
10. *Advanced Encryption Standard (AES) (FIPS PUB 197)*. "National Institute of Standards and Technology (NIST)", (Nov 2001).
11. T. Issariyakul, E. Hossain, *Introduction to network simulation ns2*, (July 2008).