ISSN:0975-9646

Wireless Multi-Domain Network: A Study of Routing Protocols and Security Enhancements

Girish Tiwari and Shalini Sharma

Department of Electronics and Communication Engineering,
Ujjain Engineering College, Ujjain, M.P. (India)

***ABSTRACT* - Several routing protocols have been proposed in recent years for deploying the wireless networks in various fields like commercial applications, government and various military operations. In this paper, we analyze and review number of routing protocols with particularly focusing on various security issues. All the existing protocols differ in terms of routing methodologies and the information used to make metric and cost calculation as well as routing decisions. The most frequently used and efficient routing protocols such as WEP, AES, IPsec, PKI etc. are discussed. To secure the wireless networks, we focus on five security requirements such as validation, non-repudiation, confidentiality, opportunity and integrity. In this paper we analyze the above mentioned protocols for the Wireless Multi-Domain Networks for the improvement purpose in terms of its security solutions.**

Keywords: WMDN, routing protocol, validation, confidentiality, integrity, inter-domain BGP.

I. INTRODUCTION

Wireless multi-domain network (WMDN) consists of multiple domain, each one made up of nodes and links. All nodes are administrated as a unit in a domain with the same rules and the procedures. Fig. 1 [1] shows a multi-domain network consisting of individual controlled domains. Each domain is controlled by its own Network Control Centre (NCC). Integrated NCC (INCC) administrates NCCs and their cooperation. In WMDN, security can be discussed on the basis of two schemes [2]: communication over a single domain in itself (intra-domain routing) and communication between domains (inter-domain routing).

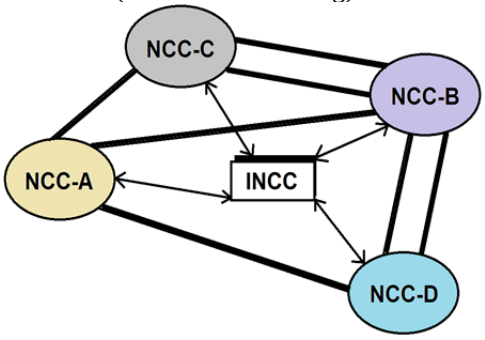

Fig. 1: A multi-domain Network

Our main concern is to discuss the routing protocols with particularly focusing on various security issues. Further, we will discuss on several threats in wireless multi-domain network and then summarize the already existing solutions against the threats. Here, we consider some properties of routing protocols [1] to design an applicable routing algorithm, and challenges while routing in WMDN.

A. Properties of routing protocols

1) *Node Independent Internet Information:* Internet information is independent of the size of respective domain and the nodes. Each node in a particular domain is not recognized by other domains and so the information is meant only to the same domain. This property entails more intensive routing protocol and destination independent routing.
2) *Loop-Free Routing:* This property offers both the inter-domain and the intra-domain routing without repeating any node, in the actual path, since each node knows about all the details of the internal structure. Each domain is controlled by Network Control Center (NCC).
3) *Destination Dependent Statistics:* Each node has details of the traffic from an internal node to an external domain. Each node reports NCC about this detail and NCC reports to the INCC about that intensive detail.
4) *Parallelism of NCC's:* To obtain the maximum affinity, each NCC needs to work independently and parallely.
5) *Cooperation:* A wireless network depends on the cooperation of the nodes present for routing and packet transmission. If the source and destination nodes are not in the range of one another, then the communication between those nodes takes place by the help of other nodes [3]. Generally, the neighboring nodes form an optimum chain of mutually connected nodes and in this type of network, each node acts like a host as well as router and so this type of communication is also known as multi-hop communication.
6) *Dynamic Topology:* In dynamic topology, different nodes may join or leave the network at any instant of time and thus this type of topology has risk of link failures and malicious attacks by some unauthorized node which may join the network at any point of time. So it is very important to secure this type of network against the malicious attacks.
7) *Absence of fixed infrastructure:* The key feature is that they lack central or fixed infrastructure. Thus it becomes difficult to establish an authority to control the network characteristics in case of Ad-hoc networks. Due to the lack of centralized authority, the traditional network management techniques and security algorithms are rarely applicable to the Ad-hoc networks.

Whether the network is infrastuctured or infrastructureless, the security requirements such as non-repudiation, validation, integrity, confidentiality and opportunity [4] remain same but due to the inherent characteristics, the infrastructureless networks are more sensitive to the security attacks [5]. Due to the open exposure of nodes and wireless channels, lack of NCC, dynamic topology etc., it becomes a big challenge to secure the infrastructureless network from the attackers [6]. Any legitimate user or malicious user intended to attack, can access the network. The absence of NCC obstructs the traditional security mechanism which is, in general, done by the NCC. The dynamic topology may allow any legitimate or malicious node to become a part of the network at any time. Those nodes can disobey the routing protocols and disrupt the cooperative communication network.

B. Challenges

In wireless network, devices participating in the communication may belong to a single domain network or to the network with different types of domain [7] and hence wireless devices need to cooperate in both the inter-domain routing and also in the intra-domain routing.

In an intra-domain routing [8], the wireless devices are considered as a set of heterogeneous element. The dynamic topology of communicating network is the major issue when inter-domain routing is provided to the Ad-hoc network. There is no fix design of the network, all the nodes are movable and therefore they may connect with different gateways or leave the range of the network or may also overlap the other one node. A single domain of network, sometime, can be divided into disconnect networks and at that time (Fig. 2), the connectivity can only be made by maintaining the connection through the roaming nodes between those disconnect networks. These properties of the inter-domain routing are directly used in the Ad-hoc networks.

One can apply the border gateway protocol (BGP) [9] to the scenario shown in the Fig. 3. The BGP provides an autonomous system (AS) which is the standard mechanism among the heterogeneous network for the inter-domain routing. However, the BGP cannot be applied because of several issues. The first one is the distance vector which assumes only if the following functions are available:

1) *Detection of Internal Gateways:* When the information comes from the external routes, internal gateways within the same domain can distinguish the existence of each other as they can know whom to communicate with.
2) *Internal Network's Knowledge:* The destination and the following route should be known to the gateways participating in communication.

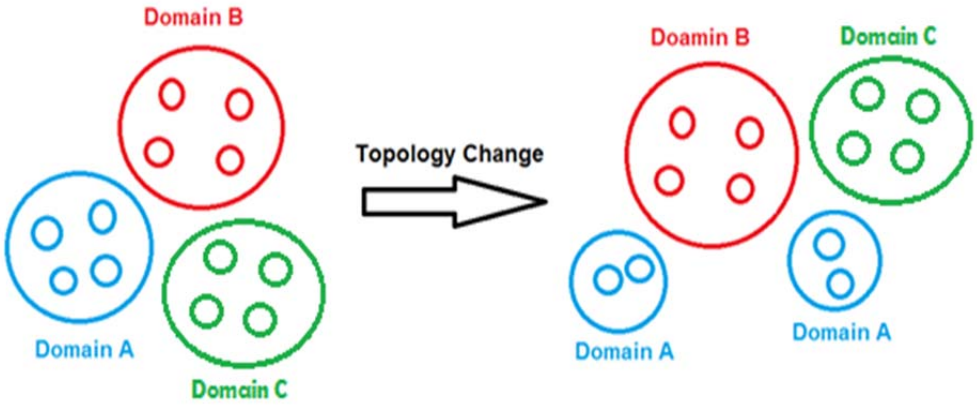

Fig. 2: Partition of Domain-A in Ad-hoc network due to the mobility of nodes

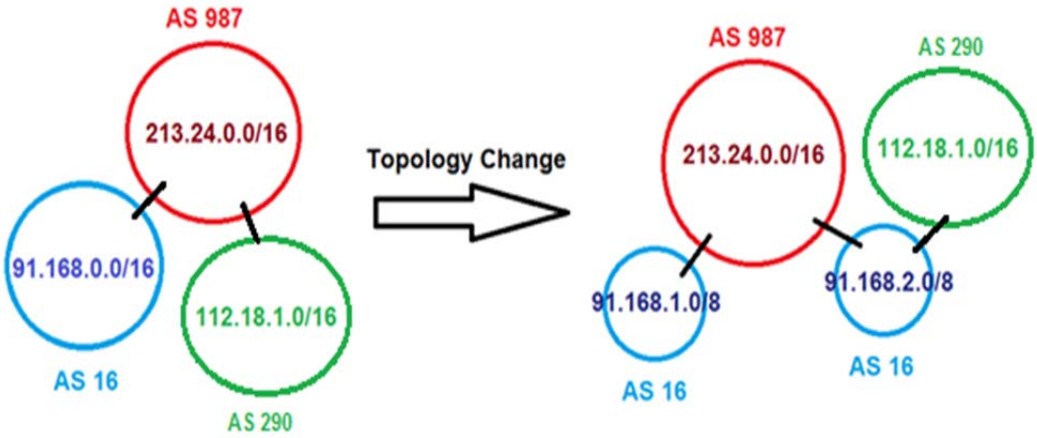

Fig. 3: Partition of Domain A in Ad-hoc network due to the change in topology

The proactive routing protocols e.g., link state routing protocol and distance vector routing protocol for intra-domain support these functions by maintaining the state information of the network. As the Ad-hoc network uses reactive or hybrid routing protocol, so we cannot assume the information availability all the time as they do not provide these functions necessarily out of their regular operation. Hence, it may be undesirable to apply a distance vector routing protocol over the Ad-hoc network to support these functions during the process while the nodes are dynamically moved and the bandwidth is limited.

Second one is that IP addresses are needed to identify the destination in BGP. Destinations in a particular domain can be revealed by the gateways in that domain by combining the IP address with the suitable IP prefixes (e.g., 91.168.0.0/16). The partition of domain does not allow the combining of IP address with suitable IP prefix, as it can create scalable routing tables.

Third, as BGP depends on the distance vector routing protocol, it provides prevention from the looping by filtering out the distance path with repeated AS e.g., after change in topology (Fig. 3), the path from source AS 16 (91.168.1.0/8) to AS 290 (112.18.0.0/16) is AS 16---AS 987---AS 16---AS 290.

II. ROUTING PROTOCOLS FOR WMDN

A. Intra-domain routing protocols

These protocols, for example: Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Intermediate System – Intermediate System (ISIS) etc., ignore the communication outside the autonomous system (AS). Based on the performance and security, since most of the protocols are based on the shortest-path algorithm, the routing measures can be considered as random preferences over the forwarding path [8]. These protocols are also called as interior gateway protocols. Hiding the deficiency of intra-domain routing protocols, the intra-domain routing protocols are used.

B. Inter-domain routing protocols

These protocols, for example: BGP assume that the communicating network consists of a group of interconnected AS's. An important component of inter-domain routing is to support the domain-level routing policies.

In BGP, intra-domain routing protocols (i-BGP) are used for determining an interior destination within the same domain, whereas inter-domain routing protocols (e-BGP) are used for determining an external destination among domains. For exchanging the information at inter-domain level, BGP depends on distance-vector protocol as distance-vector protocol has an advantage that it is easy to determine the preference route selection by implementing a policy based routing in domain administrator.

Each domain in the internet has a particular identifier called AS number. Distance-vector protocol maintains a list of AS number of crossed domains, so that the route to the specific destination can be filter and selectively announced by each domain. Design of a BGP depends on many expectations such as (i) Gateways have complete knowledge of the destination independent of information transmission (proactive intra-domain routing), (ii) BGP gateway depends on IP-prefix to reduce the size of routing tables and (iii) Identification of AS number detects loop in the inter-domain topology.

III. THREATS IN WMDN ROUTING

In an intra-domain routing infrastructure, there are two types of user: (i) Insiders: they are legitimate users who have either limited or unlimited access to the routers and (ii) Outsider: they are external to the network and they can do harm to an intra-domain routing infrastructure by causing network routing to malfunction in one way or the other [10].

	Acquiring routing information (ARI)	**Denial of service (DoS)**	**Routing-path manipulation (RPM)**
Outsider	1. Sniffing 2. Traffic analysis-Network Tomography	1. Interference a) Add noise b) Inject dummy routing/data traffic c) Replay old packets	1. Can manipulate
Insider	All capabilities of outsiders	All capabilities of outsiders	
Insider	1. Routing analysis 2. Deliberate exposure	1. Interference a) Not forwarding packets b) Delay responses c) Inject wrong routing packets 2. Overload a) Overload CPU b) Overload link-state database	1. Impersonation 2. Falsification a) Claim non-exist links b) Disclaim exist links c) Modify, insert, or substitute routing message

Table 1: Threats in WMDN Routing

An attacker may be an insider or an outsider. The type of threats can be classified based on the condition that it is initiated by an insider or an outsider:

A. Threat possibilities from outsider

1) Acquiring routing information (ARI):

a. Sniffing: An outsider can monitor or record the routing exchanges between the authorized routers to detect (sniff) for the routing information and thus after acquiring the routing information, it can make the network routing to malfunction.

b. Traffic Analysis: An outsider may measure the end to end performance of the network (e.g. the number of packets sent or received or the time delays between the sent and the received packets) and based on this statistical analysis; it can make the routing path to malfunction.

2) Denial of Service (DoS):

a. Interference: An outsider may block the routing exchanges between the legitimate routers to disrupt the routing information by adding noises or by injecting dummy data or routing packets.

3) Routing Path Manipulation (RPM):

By acquiring the routing information, an outsider can change the desired routing paths.

B. Threat possibilities from insider

For making an attack, an insider has some additional capabilities than an outsider which may be listed as follows:

1) Acquiring Routing Information (ARI):

a. Routing Analysis: An insider has always more routing information than an outsider so it can harm the network easily (if it wants).

b. Deliberate Exposure: An insider can sometime intentionally release routing information to others such as outsiders or to others who are not authorized to receive the exposed information.

2) Denial of Service (DoS):

a. Interference: An insider can sometime drop the received routing packets or delay the responses of the received routing packets or inject wrong routing information to prevent other routers from making correct routing tables.

b. Overload: An insider can sometime place excess burden on other legitimate routers so that they are unable to make their routing table.

3) Routing Path Manipulation:

a. Impersonation: Sometimes, an insider can act like two or more virtual router at a time, thus creating a shorter path for the packets to attract data traffic or creating a longer path to expel the data traffic which may lead to falsification.

b. Falsification: An insider may sometime create shorter or longer path between the communication channels to deviate the data traffic to a host controlled by an attacker.

In summary, the threat possibilities which we have discussed so far are ARI, DoS and RPM. The three main aspects of a secure network are confidentiality (related to ARI), integrity (related to DoS) and availability (related to RPM).

IV. POSSIBLE SOLUTIONS

In this section, we will discuss about the security measures, already existing as the solutions developed in past few years, to provide security against the threats in WMDN.

A. Wired Equivalent Privacy

WEP is a security algorithm which is introduced as a part of IEEE 802.11 standard [11]. It provides data confidentiality by giving the same password to everyone) [12]. WEP standard uses a 64/128/152/256-bit key [13] [14] [15]. This key is the combination of 24-bit initialization vector (IV) and 10/26/32/58 digits, respectively, of 4-bit hexadecimal characters (0-9, A-Z). WEP uses two authentication methods: Open authentication and Shared key authentication. Any user can access the open authenticated network. In shared key authentication method, user needs to follow the four step challenge-response handshake. Shared Key method gives more security but open authentication method is advisable for privacy concern.

B. Advanced Encryption Standard

AES is an excellent and balanced algorithm which gives better security with efficient performance, flexibility and ease of implementation. It provides a subjective encryption scheme combined with the cryptographic modes operation [16].

Ferguson et al. [17] have proposed some algebraic properties that the security of Rijndael algorithm [18] is dependent on computational assumptions. AES cannot solve all the problems of cryptography such as it reveals the key when substitutes RC4 in WEP. Due to this, AES may reveal additional vulnerability and even insecurity.

C. Network Layer Security & IPsec

IPsec is the standard which gives the security at the network level by providing validation, integrity and confidentiality. IPsec provides security between two trusted networks by dividing the IP packets into three segments a) at the sender end network, b) at untrustworthy public network and c) at the receiver end network. Because of this untrustworthy public network, IPsec gateways are required to place between trustworthy and untrustworthy networks. It provides validation, integrity and confidentiality by employing the three protocols: Internet Key Exchange (IKE) [19], Authentication Header (AH) [20], and Encapsulation Security Payload (ESP) [21] respectively.

D. Public Key Infrastructure

PKI is based on the public key cryptography which utilizes a pair of private and public key [22]. A third trusted party called Certification Authority (CA) [23] generates a certificate by using its private key which is used to combine a particular entity's identity with the corresponding public key. Using the public key, it provides non-repudiation, validation, integrity and confidentiality. It facilitates a secure exchange and storage of electronic information, ensuring the safety by using the public key. In PKI, security is achieved by reversing the order of the key. PKI is used to secure web services, emails, authentication systems and virtual private networks. In PKI, it is very important to

ensure the efficiency and the performance when we work on the multi-domain network.

E. Solution to Link State routing attack

Dijiang Huang et al. [10] have proposed a mechanism which reduces the effect of DoS attacks. It prevents insider from impersonation and forging the information by offering confidentiality, integrity and validation to the legitimate node. It provides the security feature that does not allow the nodes to change the operational functionalities of the routing protocols. The mechanism proposed can be applicable to the intra-domain routing. This proposed mechanism is depends on the confidentiality and the validation at information level. It also focused on balance between cost issues and performance/security of network.

F. Solutions to the Flooding Attack

P. Yi et al. [24] have proposed a mechanism to secure the AODV protocol from the flooding attack. Neighbors' RREQ are monitored by each nodes, these nodes have a blacklist containing the ID of those neighbors whose RREQ rate exceeds the predefined threshold. The further RREQs from those blacklisted neighbors are dropped. The demerit of this approach is that it sometime allows the attackers when attackers' RREQ rate is not exceeded and does not allow the legitimate node when its ID is copied by another malicious node which tries to send a large number of RREQs.

S. Desilva et al. [25] have proposed a technique which can adapt by the AODV protocol to reduce flooding attack's effect. It avoids forwarding the packet by statistical analysis when malicious RREQ floods are detected. This approach gives an advantage for varying flooding rates that it reduces the effect of attacks.

G. Solutions to the Black-hole Attack

P. Jaiswal et al. [26] have proposed that the sender nodes sends a request packet to the next hop node and wait for the replies from next hop node with the details of other neighboring nodes. A timer is set after the reception of first request for collecting the other requests from different neighboring nodes. The timeout period is measured from the time the first request received. The packet sequence number and time of packet receipt is stored in the Collect Route Reply Table (CRRT). CRRT is used to check the repeated next hop node. A random route is selected from CRRT when no repeated node is found.

Lee et al. [27] have proposed two packets: CREQ (route confirmation request) and CREP (route confirmation reply) to prevent from the black-hole attack. The source node sends the CREQ to next hop node towards the destination. The next hop node sends CREP to sender when a route is found. After receiving the CREP, sender checks the path content in both the CREP and RREP, when found same path content, it announces that the path is correct to follow. In this proposed work, the black-hole attack is not solved as if the next hope assumed to be illegal attacker.

M. A. Shurman et al. [28] have proposed that source node need to wait until it receives the RREP packet from three or more nodes. Then it checks the hop who shares the packet after receiving those packets. The route is pretend to safe by the source node when the packet is coming from at least one hop. The demerit countable here is that the waiting for packets by the source node may introduce time delay.

V. CONCLUSION

Wireless multi-domain network, now a day, is an emerging technology in network field which needs to be analyzed and discussed. In this paper, we have discussed about several routing protocols for multi-domain wireless networks and also considered their security issues with the concern of five security requirements such as validation, non-repudiation, confidentiality, opportunity and integrity. The solutions for the improvement of security were also discussed in this paper. There is always a tradeoff between the security measures taken and the cost of implementation. So we must always keep in mind the application area of our routing protocols. The insight study will definitely guide us to identify the new areas of research and also to enhance and secure the already existing routing protocols against the mentioned security threats in the wireless multi-domain networks.

REFERENCES

[1] Dragomir D. Dimitrijevic, Robert R. Boorstyn, "*Routing In Multidomain Networks*", IEEE/ACM Transactions on Networking, Vol. 2. No. 3, June 1994.

[2] L.D. Chen, G. Gong, "*Network Domain Security*", Communication System Security, Chapter 3, 2008.

[3] K. Muthukumaran, D. Jeyakumar, C. U.Omkumar, "*A Concise Evaluation of Issues and Challenges in MANET Security*", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 9, September 2013.

[4] A.Weimerskirch and G.Thonet, "*Distributed Light-Weight Authentication Model for Ad-hoc Networks*", Lecture Notes in Computer Science, Springer; Vol. 2288, pp. 341 354, 2001.

[5] I.Chlamtac, M.Conti, and J.Liu, "*Mobile Ad Hoc Networking: Imperatives and Challenges*", Ad Hoc Networks, vol. 1, no. 1, pp. 13- 64, 2003.

[6] J.P.Hubaux, L.Buttyan, S.Capkun, "*The Quest For Security In Mobile Ad Hoc Networks*", Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), October, 2001.

[7] www.webopedia.com/TERM/D/domain.html.

[8] Chi-Kin Chau, Jon Crowcroft, Kang-Won Lee, Starsky H.Y. Wong, "*IDRM: Inter-Domain Routing Protocol for Mobile Ad Hoc Networks*", University of Cambridge Computer Laboratory, no. 708, January 2008

[9] A.Iwata, C.C.Chiang, G.Pei, M.Gerla and T.W.Chen, "*Scalable Routing Strategies for Ad Hoc Wireless Networks*", IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1369-1379, August 1999.

[10] Dijiang Huang, Qing Cao, Amit Sinha, Marc J. Schniederjans, Cory Beard, Lein Harn, Deep Medhi, "*Addressing Intra-Domain Network Security Issues through Secure Link-state Routing Protocol: A New Architectural Framework*", accepted by Communications of The ACM, April 2005.

[11] IEEE Std 802.11-1997 Information Technology- telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications, 1997.

[12] Vacca, J. R., "*Types Of Wireless Network Security Technology*", Guide to Wireless Network Security, 2006, xxiv, 848 p. 63 illus, Hardcover, Springer.

[13] http://www.informit.com/guides/content.aspx?g=security&seqNum=85.

[14] An Inductive Chosen Plaintext Attack against WEP/WEP2". cs.umd.edu. Retrieved2008-03-16; http://www.cs.umd.edu/~waa/attack/v3dcmnt.htm.
[15] IEEE 802.11i-2004: Medium Access Control (MAC) Security Enhancements.
[16] Morris Dworkin, "*Recommendation for Block Cipher Modes of Operation, Methods and Techniques*", National Institute of Standards and Technology, 2001
[17] Neils Ferguson and Bruce Schneier, "*A Cryptographic Evaluation of IPsec.*", http://web.cs.wpi.edu/~rek/Adv_Nets/Spring2002/IPSec.pdf.
[18] N. Ferguson, R. Schroeppel, D. Whiting, "*A Simple Algebraic Representation of Rijndael*", 8th Annual Workshop on Selected Areas in Cryptography, pages 103–111, 2001.
[19] D. Harkins, D. Carrel, "*The Internet Key Exchange (IKE)*", Network Working Group, November 1998.
[20] S. Kent, R. Atkinson, "*IP Authentication Header*", Network Working Group, November 1998.
[21] S. Kent, R. Atkinson, "*IP Encapsulating Security Payload (ESP)*", Network Working Group, November 1998.
[22] Muhammad Sher, Thomas Magedanz, "*Developing Network Domain Security (NDS) Model for IP Multimedia Subsystem (IMS)*", Journal of Networks, Vol. 1, No. 6, November/December 2006.
[23] Imran Ijaz, "*Design and Implementation of PKI (For Multi Domain Environment)*", International Journal of Computer Theory and Engineering, Vol. 4, No. 4, August 2012
[24] P.Yi, Z.Dai, S.Zhang, Y.Zhong., "*A New Routing Attack In Mobile Ad Hoc Networks*", International Journal of Information Technology, vol. 11, no. 2, pp. 83-94, 2005.
[25] S.Desilva, and R.V.Boppana, "*Mitigating Malicious Control Packet Floods In Ad Hoc Networks*", Proceedings of IEEE Wireless Communications and Networking Conference 2005, , vol. -4, pp. 2112- 2117, March 2005.
[26] P. Jaiswal, R. Kumar, "*Prevention of Blackhole Attack in MANET*", International Journal of Computer Networks and Wireless Communications,Vol.2, No5, October 2012.
[27] S.Lee, B.Han, and M.Shin, "*Robust Routing in Wireless Ad Hoc Networks*", 2002 International. Conference on Parallel Processing Workshop, Vancouver, Canada, pp. 73-78, August 2002.
[28] M.A.Shurman, S.M.Yoo, and S.Park, "*Black Hole Attack in Mobile Ad Hoc Networks*", ACM Southeast Regional Conference, pp. 96-97, 2004.