J. Basic. Appl. Sci. Res., 3(3)101-107, 2013

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Security Enhancement of Pro-active Protocols in Mobile Ad-hoc Networks

M .Nasir Iqbal, Junaid A.Khan, Farooq Umer, Nadeem Javaid, Izhar-ul-Haq, Mustafa Shakir

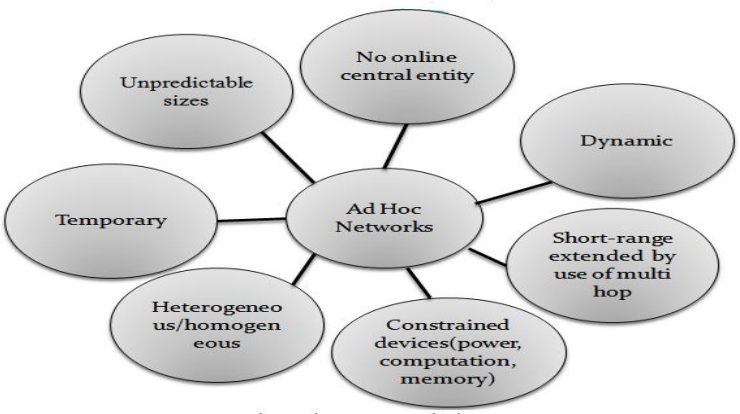
Department of Electrical Engineering, COMSATS Institute of Information Technology, Islamabad

ABSTRACT

Security of node is an essential task in MANETS. Mobile Ad Hoc network is constructed of mobile nodes which communicate with other nodes through any wireless medium without any fixed infrastructure. Due to dynamic network topology routing in (MANETs) is a critical task due to highly dynamic environment. Security is the basic need of Ad-Hoc networks for secure communication between mobile nodes. We introduce a security scheme for pro-active (table-driven) protocols. In this security scheme we use an even-odd function .In this function each node will generate either even or odd random number during signaling period and reverse the order of even-odd numbers after reaching the destination node. The advantage of this security scheme is to protect from any intruder or outsider node to attack or capture the node of the wireless network. We use even-odd function to make the network more secure for proactive protocols in MANETs.
KEYWORDS: MANETs, Pro-active protocols, Ad-Hoc, Security extensions.

1. INTRODUCTION

The most demanding technology now a days is Mobile Ad Hoc Networks (MANETS). Ad hoc wireless network consists of nodes which communicate with other nodes through wireless medium without any fixed infrastructure shown in (*figure .2*).In this figure there are three nodes in the network ,source node, intermediate node and destination node. Each node worked as peer-to-peer mode and considers as independent router and generates independent data. In [1] author describes the characteristics of mobile ad-hoc networks. Ad-hoc network topology is dynamic, self-organization, self administration. Network topology changes at any time by entering or leaving of node. Due to high mobility of nodes the network topology may change quickly and unpredictably. There is no central entity in Ad-hoc wireless network , so nodes have to discover the topology and deliver the messages generated by all nodes. It is a multi-hop wireless network with limited physical security shown in (*figure 3*).In figure 3 a node can use multi-hops to transmit a data from source to the destination. There is no default router or node present so each node works as router and transmit packets to other nodes to enable information sharing between mobile nodes. There are three main components or resources of node are battery, memory, and computation. Batteries present in each mobile node limit processing power so battery life should be better especially in war scenarios. This is the worst problem in MANETs because a node performs the duties as end system and router. Additional energy is required to forward packets from other nodes. Ad–hoc wireless network is scalable. In network topology all nodes broadcast Hello massages in the network topology to get information of their neighboring nodes while signaling period. All characteristic of Ad-hoc network discussed in this paragraph is shown in Fig.1. [8].



Wireless Ad Hoc Network characteristics
Figure . 1

***Corresponding Author:** Mustafa Shakir, Department of Electrical Engineering , COMSATS Institute of Information Technology, Islamabad. mustafa.shakir@comsats.edu.pk

1.1 application of manets

MANETs are of vast usage in different kinds of communication networks. [3]. Military networks are made to maintain a low probability of intercept and a low probability of detection. Different applications have different type of wireless network topology. Military also employs tactical networks in Ad-hoc wireless in its communication system. It also plays a critical role in communication during operations and assaults against the enemy. It is also utilized in automated battlefields. Due to its characteristic of easy mobility it's a most effective communication tool for search and rescue services. During the natural disasters for example floods, storms whereby fixed communication structures are destroyed, then the wireless Ad-hoc network can efficiently fill the vacuum of communication loss. Now a days corporate working style is in place in most of the big companies/firms. This ad-hoc network also fits in such offices. Ad-hoc network may becomes a part of 4G architecture in near future. This 4G technology provides user friendly environment that helps users to completing different tasks from anywhere from any device.

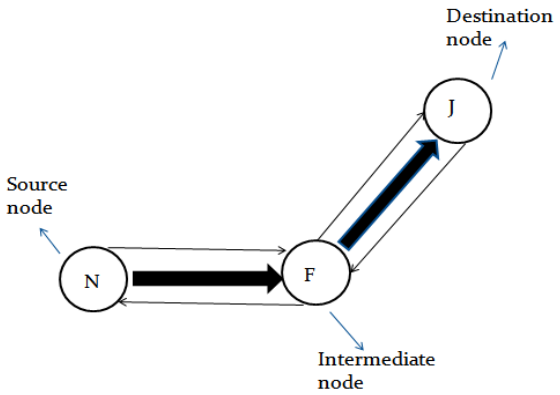


Figure 2: Network topology

In this paper section 2 is written about addressing of nodes that how to address the nodes for communication. In this paper Section 3 is about routing protocols for MANETs and about the metrics for selecting the best routes. Functioning of pro-active protocols are discussed in section 4.Then in section 5 we will discuss about the major attacks on the MANETs includes impersonate, modification, flooding and black hole attack. After this we will talk about the method of security in section 6. Security is an important issue for Ad-hoc networks, especially for those sensitive- applications and in last section 7 we will discuss a new adopted idea for securing the Ad-hoc network by using some scheme named as even odd function and in last we will discuss the conclusion in section 8.

2. Addressing

In [1] author tells about the addressing of mobile node in a wireless network. Address information would be required by every node for wireless contact between nodes in Ad-hoc wireless network. If there are two networks that are far way uses IP address for communication. MAC address can also be used if the communication is required within the network. Now a days we are using TCP and UDP for communication. TCP stands for *Transmission Control Protocol* which is more reliable because of ACK. and UDP stands for *User Datagram Protocol* and lack of ACK. It is mostly used in voice and video data streaming in the network.

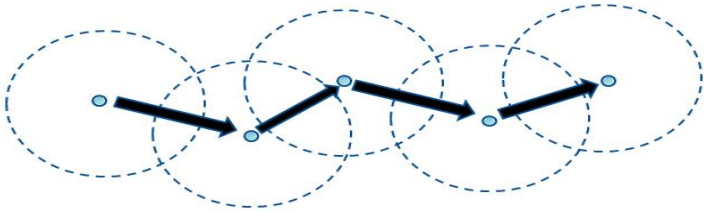


Figure 3 : Multi-hoping in MANETs

3 . Routing Protocols for MANETs

For enabling wireless communication in Ad- hoc networks, different routing protocols are used to discover routes and find the MAC addresses between Ad- hoc wireless nodes. The important goal of ad-hoc network routing protocol is to make optimum and fastest route establishment between mobile nodes so that message reached to the destination in time. The best route in Ad-hoc wireless communication is that in which bandwidth consumption and overhead is less. In ad-hoc networks, there is lack of topology information so that nodes have to discover the topology by sending hello messages within the network. In [2] author has proposed that when new node enters the topology it announces its presence within the network and listens to broadcast announcements from its neighbors.

Routing algorithms have to:

1. Keep routing table reasonably small.
2. Choose best route for given destination includes fastest, highest throughput, reliable.
3. Keep table up-to-date when nodes leave, move or join.
4. Small amount of messages/time is required to converge.

3.1 Routing Metrics

Ad-hoc networks usually consider the hop count as a routing metric. In [4] author tells about the metrics importance for ad-hoc networks For selecting best path or route for communication in wireless Ad-hoc network we consider some metrics are as under. In [6] author tells about the metrics and cost of links between mobile nodes.

1. Path Length
2. Reliability
3. Delay
4. Bandwidth
5. Load
6. Communication Cost

4. Functioning Mechanism Pro-active Protocols

Proactive protocols are table-driven protocols. In this type of protocols communication delay is less than reactive protocols.

Each node or system maintains a table in its memory device.

Every system or node sends a Hello message to get the information of entire network topology. Before establishing network each node knows the node IDs of other neighboring nodes. There is less delay in sending data from source to destination nodes in pro-active protocols. Examples of pro active protocols are as under in (table 1).

[1]	DSDV
[2]	WRP
[3]	CGSR
[4]	STAR
[5]	OLSR
[6]	FSR
[7]	HSR
[8]	GSR

Table 1: Pro-active Protocols

4.1 An Overview of Proactive protocol

An overview of proactive protocols [7] is as under:

a) Link-state routing protocol.

b) (Table-driven) Three main components:

1. Neighbors Sensing mechanism.
2. Broadcast forwarding/flooding mechanism.
3. Topology Discovery (diffusion) mechanism.

4.2 Protocol Dependent on Routing information update

Routing protocols which operate with the help of routing information update mechanism is shown in (figure 1.4).Reactive, pro active and hybrid protocols are the types of routing information update mechanism [10].

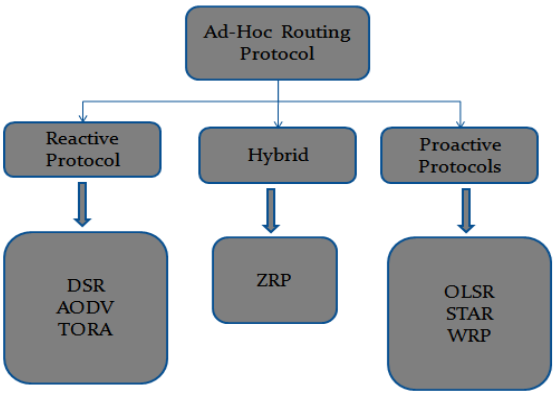


Figure 4: Ad-hoc Routing Protocols

5. Attacks on OSI Layers on MANETs

In [5] tells the attack on different layer of OSI model. Mostly intruder or outsider node attacks the network layer to capture the infrastructure mobile node .Due to high mobility of nodes chances of attacks increased. Different types of attacker's attacks on different layers during wireless communication (set of functions) are as follows:

Application layer : Malicious code, Repudiation

1. Transport layer : Session hijacking, Flooding
2. Network layer: Flooding, Black hole, link spoofing.
3. Data link layer : Active , passive, malicious behavior
4. Physical layer: Traffic jamming.

5.1 Most Important Attacks in MANETs and routing protocols

Two types of attacks on routing protocols are as follows.

1) Routing disruption attacks.
2) Resource consumption attacks.

In first kind of attack, packets would be sent on wrong paths of the wireless network. This act allows the attacker to utilize the network bandwidth. Attack is carried out when nodes try to transmit false packets on pre-designated network paths.

I depict a broader classification of the possible attacks in MANETs are as under.

a) Impersonate
b) Modification
c) Flooding attack
d) Black hole attack

5.1.1 Impersonate Attack

Impersonate attack is a dangerous threat to the security of mobile ad- hoc networks. If there is no proper mechanism of authentication between mobile wireless nodes .Bad node can enter easily in the wireless network and acts as a part of network. Then bad node behaves maliciously and transmits wrong messages to the entire network and safe wireless communication is not possible. In this attack node can gain inappropriate priority to access some confidential information. This is dangerous for wireless communication. Example of impersonate attack is shown in (figure 5) in which two nodes 1 and 2 are the malicious node in the network.

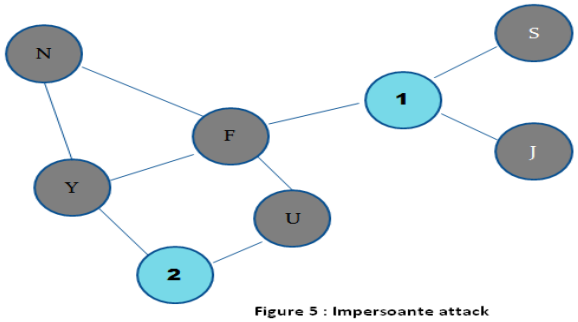


Figure 5 : Impersoante attack

5.1.2 Modification Attack

Malicious node in modification attack in wireless communication changes the routing message by including wrong information in data packets .It affects the integrity of the data packets in the network. Due to high mobility of nodes there is great chance of entering of malicious node in the network topology.

5.1.3 Flooding Attack

In flooding attack attacker exhausts the battery, memory and computation of the node in the network. These are the important and essential resources of node in an Ad hoc wireless network. Flooding attack decrease the efficiency of network by consuming bandwidth by sending useless messages in the entire network.

5.1.4 Black Hole Attack

This attack is carried out by a culprit node after claiming possession of an optimum route. The culprit node sends the deceptive message to whole network topology. This results in pressing the good nodes to send the data through the culprit node. In this way malicious node can misuse the important information of the network especially in war conditions. Example of black hole attack is shown in (*figure. 6*). In this figure node A is the outsider or malicious node and acts as a part of network and claim that it has an optimum route to the destination.

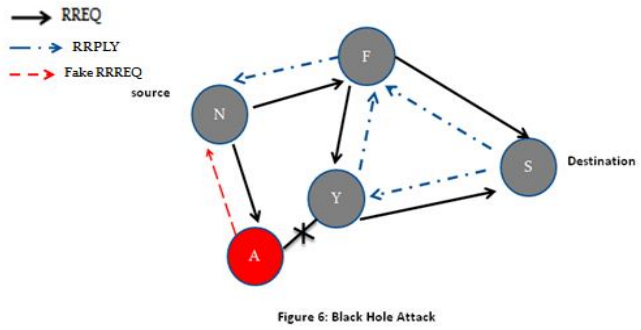


Figure 6: Black Hole Attack

Figure .6 Black Hole Attack

6. Need for Security and prevent against Attacks

Security is the basic need for secure communication between mobile nodes in a hostile environment. Security is the main part of the wireless network. Different security mechanism are introduced in wireless network field to protect from different attacks on MANETs which includes impersonate attack, modification attack, flooding attack and black hole attack were discussed in section 5 in this paper. lot of work on security of ad hoc wireless network is done in recent years because of its self-configuration and self maintenance properties. [9]

6.1 Secure and Safe Routing for Ad-hoc networks

Ad-hoc network should react very quickly when any attack is launched on the wireless network and any abrupt change occurs in the topology. In any case if malicious node attacked on the network successfully, implemented security mechanism should take measures to make the network secure and safe as soon as possible. Protocols that are designated for Ad –hoc networks performs well in dynamically changing networks.

Two main sources of threat to the routing protocol are external attackers and the second is compromised node. In the first source of threat (external attackers) attacker will try to inject wrong routing information and also try to make separation in the network topology. Sometimes attacker successfully makes partition in the wireless network topology with this first source of attack. In second and also the more dangerous kind of threats come from compromised nodes. In this type of threat node advertise fake routing information to other nodes in the network topology. Compromised nodes are also able to generate the valid signature using their private keys. There are two methods to prevent the network from these threats by cryptographic schemes which includes digital signature.

7. Adopted Authentication Approach for Network Security

Security is the most important part of the wireless ad- hoc networks. While communication between nodes, secure communication is necessary in wireless infrastructure less network in a hostile environment .In this paper we are going to introduce a new idea to secure wireless Ad-hoc network through a different scheme. A security scheme for pro active (table-driven) protocols In this scheme we use [even- odd function].

In this scheme the transmitting node transmits a unique ID with random even or odd number to the receiving or its neighboring nodes. The whole idea is discussed in the (*figure 7)* shown below. In this scheme each node is assigned a unique

ID before creating a wireless network for communication between nodes .when a wireless network is established and node (N) wants to communicate with node (J) in the network topology. The node (N) acts as a transmitting node ,it will send a message during signaling period with unique node ID and generate a random odd number for example 3.when this message is broadcast to its neighbors. Receiving node for example (A) first verify that is has an ID

of transmitting node in its routing table. If it exists in the routing table it will accept the message from the transmitting node. If receiving node (A) is not the destination then it broadcast the message again. The node (A) will transmit a message with its unique ID and it knows that node (N) generated a random odd number so after computation using even-odd function it will generate an even number .When the destination node (J) will receive the unique ID with a random odd number. The destination node (J) will send back and reverse back the order of all the random number generation.

When the destination node(J) sends its unique ID and generate an odd number which was generated by node (T).Node (T) knows that it generated an odd number 11 then it will accept it .Same procedure is followed in the whole network till it reaches to the source node (A). After this signaling process route is established between the source node to the network node in secured environment. In this technique data is transmitted safely without any intruder attack.

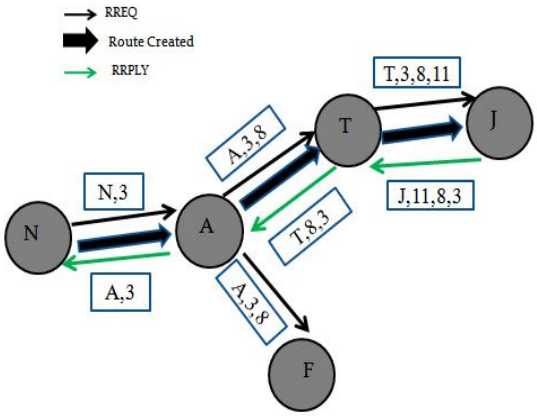


Figure. 7 : A New Idea to Make Network Secure

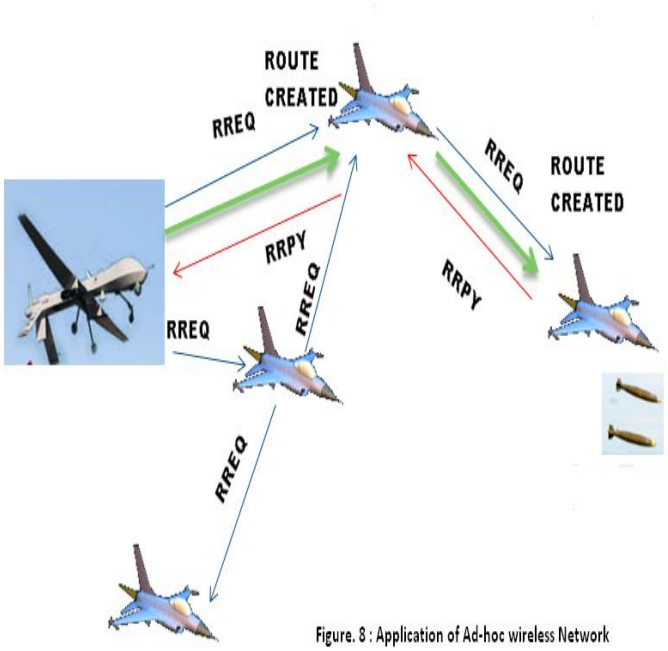


Figure. 8 : Application of Ad-hoc wireless Network

8. Conclusion

Authentication is the key to make the wireless network more and more Secure for any kind of application. By developing such schemes for MANETs encourages us making new inventions in this wide wireless field .We can transmit data efficiently with more security .We can move our all the devices on wireless especially on Ad-hoc wireless technology. This technology makes the world more global village.

In this paper, we introduce adopted authentication approach for protecting our Ad-hoc wireless network by even- odd function. In this function mobile node will compute and generates random even or odd number during signaling process. If first node generates random odd number then next node will do computation and generates random even number by incrementing of decrementing digit numbers. There are number of attacks existing in wireless communication in different application of communication field. This scheme will secure the whole wireless network from the outsider attack. In this way a secure and efficient Ad-hoc wireless communication is possible between different nodes in different scenarios. This technology is mostly used war scenarios now a days. Ad-hoc wireless technology is used in drone attack now shown in figure 8.Efficient and fast information can be send from one system to another system in a very secure mechanism by using such security schemes in Ad-Hoc wireless networks. This new adopted idea will motivate other researchers to invent new ideas for security, which is an important task in Ad-hoc wireless communication. We can use this technology in education by interacting student laptops for sharing data and communication. We can use this technology (Ad-hoc wireless network) for controlling and tracking new cars running on road. This new idea is can be implemented easily. So mobile ad-hoc networks are the future of the wireless networks because they are practical ,easy to be implemented, easy to use and are inexpensive.

REFERENCES

[1] Jeroen Hoebeke, Lngrid Moerman, Bart Dhoedt and Piet Demeester (An Overview of Mobile Ad Hoc Networks: Applications and challenges) Deparment of Information Technology (INTEC),Ghent University –IMEC vzw . Sint Pietersnieuwstraar 41, B-9000 Ghent, Belgium.

[2] Donatas sumyla (Mobile Ad- Hoc Networks (manets).

Ram Kumar Singh, Vijay Dev Saxena (Mobile Ad-Hoc Networking: An Approach, Electrinics & Communication Engg. Department Krishna Institute of Engineering & Technology..

[3] Advance Network Technologies Division, itl Wireless Ad Hoc Networks http://www.antd.nist.gov/wahn_mahn.shtml

[4] Miguel Elias M. Campista, Diego G.Passos Pedro Miguel Esposito, Igor M. Moraes GTA/COPPE/POLI, Universidade Federal do Rio de Janeiro P.O. BOX 68504-21945-970 Rio de Janeiro, RJ, Brazil

[5] Mobile ad hoc networks http://en.wikipedia.org/wiki/Mobile_ad_hoc_network

[6] Routing overview, Motorola mobility http://networking.ringofsaturn.com/IP/Routing.php#_Toc471493318

[7] Pro active protocol preview http://www.soi.wide.ad.jp/class/20030000/slides/05/47.html

[8] ECIT ,The Institute of Electronics, Communications and Information Technologyhttp://www.ecit.qub.ac.uk/Research/System-on-

[9] Lidong Zhon, Zygmunt J. Haas,Department of computer Science, School of Electrical Engineering, Cornell University, Ithaca, NY 14853

[10] Kathryn Higgins, Ruth Egan, Shonagh Hurley *and* Marine Lemur *ad hoc networks*