Significance of Mobile AD-HOC Networks (MANETS)

Aditya Bakshi, A.K.Sharma, Atul Mishra

Abstract- Wireless networks use radio frequencies in air to transmit and receive data instead of using some physical cables. Wireless networks are formed of routers and hosts. In a wireless network, the routers are responsible for forwarding packets in the network and hosts may be sources or sinks of data flows .The fundamental difference between wired and wireless networks is the that the networks components communicate. A wired network relies on physical cables to transfer data. In a wireless network, the communication between different network components can be either wired or wireless. Since wireless communication does not have the constraint of physical cables, it allows a certain freedom for the host and/or router in the wireless network to move. This is one of the advantages of a wireless network.

Keywords:1.Communication 2.Wireless 3.Network 4. Mobile 5. MANET

I. INTRODUCTION

Network Components in a wireless network communicate with each other using wireless channels. The use of wireless networks has become more and more popular. Based on the type of network infrastructure used for communication, wireless communication network are categorized into two types:

- Infrastructured Networks
- Infrastructure-less Networks

Infrastructured Networks

An infrastructure network consists of wireless mobile nodes and one or more bridges, which connect the wireless network to the wired network as shown in figure 1.1. These bridges are known as base stations. A mobile node within the network searches for the nearest base station connects to it and communicates with it.

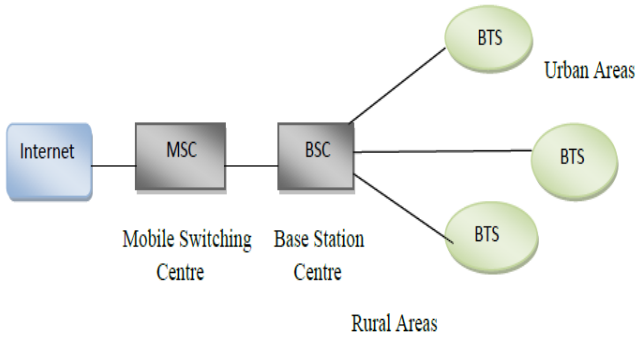

Fig 1.1 Infrastructure based network

Manuscript received on March, 2013

Aditya Bakshi, Assistant Professor, Department of Computer Science Engineering Lovely Professional University, Jalandhar, Punjab India.

Dr.A.K.Sharma, Chairman and HOD, Department of Computer Science Engineering, YMCA University of Science and Technology, Faridabad, Haryana India.

Dr.Atul Mishra, Associate Professor, Department of Computer Science Engineering, YMCA University of Science and Technology, Faridabad, Haryana India.

Infrastructure-less Networks

In Contrast to infrastructure networks, each node in this network acts both as a router and a host. The network topology is dynamic, because the connectivity among the nodes may vary with time due to node improvements. There is no base station or access point. Nodes can communicate with each other by forming a multi hope route as shown in figure 1.2. Hence there is a need for efficient routing protocol to allow the nodes to communicate over multi-hop paths without access point. Since these networks pose many complex issues, there are many problems for research and contributions. Mobile Ad-Hoc Networks is a type of infrastructure less networks in which nodes are portable devices such as mobile phones and laptops.

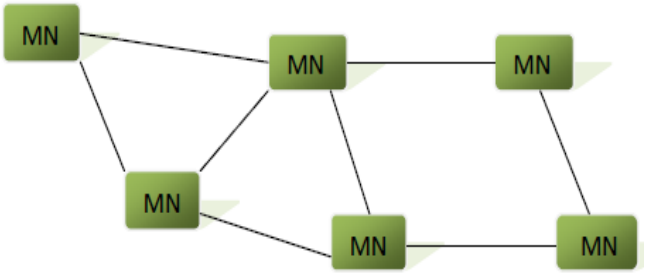

Fig 1.2 Infrastructure less network

II. MOBILE AD-HOC NETWORKS (MANETS)

The increasing use wireless portable devices such as phones and laptops is leading to the possibility for spontaneous or ad hoc wireless communication known as Mobile Ad Hoc Networks (MANET). A mobile Ad hoc network (MANET) is a self-configuring network that does not require any pre-existent (fixed) Infrastructure, which minimizes their deployment time as well as cost. As each node in this network is free to move which makes the network to change its topology continuously. These infrastructure-less mobile nodes in ad hoc networks dynamically create routes among themselves to form own wireless network on the fly as shown in Fig 1.3. Mobile Ad-Hoc Network (MANET) is one of the most active research topics during the last ten years. With the advances in wireless technologies and development of mobile devices, ad hoc networks will play an important role in enabling present and future communication. For both video and data communication, mobile radio technologies has experienced a rapid growth. A MANET is a dynamic wireless network formed by a set of mobile hosts which communicate among themselves by means of the air without any pre-existing infrastructure. Each node in the MANET can act as a router as well as host. In order to maintain connectivity in a mobile ad-

hoc network all participating nodes have to perform routing of network traffic.

The success of communication highly depends on other nodes cooperation. Therefore, MANET has the property of rapid infrastructure-less deployment and no centralized controller which makes it convenient to people and vehicles can thus be internet-worked in areas without a pre-existing communication infrastructure or when the use of such infrastructure requires wireless extension. By extending range of mobile nodes ad hoc networks supports multi-hop routing by which they can extend the range of wireless networks. Range depends upon the concentration of wireless users.

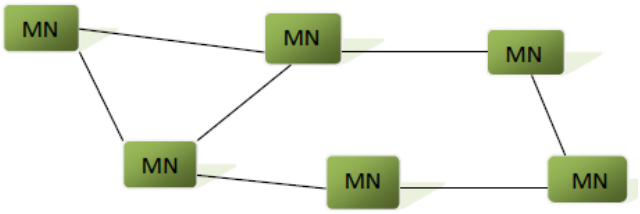

Fig 1.3 Mobile Ad-Hoc Networks

III. CHARACTERISTICS OF MANET

Mobile ad hoc network is a collection of autonomous and mobile elements such as laptop, smart phone, tablet PC etc. The mobile nodes can dynamically self-organize in arbitrary temporary network topology. There is no preset infrastructure thus it does not have the clear boundary. Some main characteristics of MANET are discussed below:

- **Infrastructure less:** MANET is an infrastructure less system which has no central server, or specialized hardware and fixed routers. All communications between nodes are provided only by wireless connectivity.
- **Wireless Links:**
  Wireless links make Mobile Ad Hoc Network unreliable and susceptible to various kinds of attacks. Because of limited power supply of wireless nodes and mobility of nodes, the wireless links between those nodes in the mobile ad hoc network are not consistent for communication participants.
- **Node Movement**
  Mobile nodes are autonomous units in network which continuously change their position and topology independently. Due to continuous motion of nodes the topology changes frequently which mean tracking down of particular node become difficult. The nodes can easily come out of or into the radio range of various other nodes. The routing information of nodes changes continuously as their movement becomes random.
- **Power limitation**
  The mobile hosts are small and light weight. They are supplied by limited power resources such as small batteries. This limitation causes vulnerability namely when attackers may target some node batteries to disconnect them, that may lead to network partition. Some attacks may try to engage the mobile nodes un-necessarily, so that they keep on using their battery for early drainage.
- **Dynamic topologies**
  Nodes are free to move arbitrarily, thus the network topology may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.
- **Self-Configuring**
  MANET has decentralized infrastructure, with all mobile nodes functioning as routers and all wireless devices being interconnected to one another. MANET is a self-configuring network in which network activities, including the discovery of the topology and delivery of messages, are executed by the nodes themselves.
- **Bandwidth-constrained and variable capacity links:**
  Wireless links have significantly lower capacity then their hardwired counterparts. Due to the effects of multiple access, fading, noise, and interference conditions, the capacity of a wireless link can be degraded over time and the effective throughput may be less than the radio's maximum transmission capacity.
- **Energy-constrained operation:**
  Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For those nodes, the most important system design criteria for optimization may be energy conservation.
- **Limited physical security:**
  Mobile wireless network are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. These characteristics create a set of underlying assumptions and performance concerns for protocol design which extend beyond those guiding the design of routing within the higher-speed, semi-static topology of the fixed internet.

IV. APPLICATIONS OF MANET

Ad hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. Ad hoc networking allows us the device to maintain connections to the network as well as easily adding and removing devices to and from the network. MANET can be applied to a large variety of use cases where conventional networking cannot be applied. MANET is used in following areas:

- **Military battlefield**
  The modern digital battlefield demands robust and reliable communication in many forms. In the battlefield it is needed by soldiers for relaying information related to situational awareness.
- **Sensor Networks**
  Another application of MANETs is sensor networks. This technology is a network composed of a very large number of small sensors. These can be used to detect any number properties of an area. Examples include temperature, pressure, toxins, pollutions, etc. Applications are the measurement of ground humidity for agriculture, forecast of earthquakes. The capabilities of each sensors are very limited, and each must rely on others in order to forward data to a central computer.
- **Disaster Area Network:**
  Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications

infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small handheld.

- **Personal Area Network:**
  Personal Area Networks (PANs) are formed between various mobile devices mainly in an ad-hoc manner, e.g. for creating a home network. They can remain an autonomous network, interconnecting various devices, at home , for example, but PANs will become more meaningful when connected to a larger network.

V. ADVANTAGES OF MANET

- **Router Free:**
  Connecting to the internet without the need for a wireless router is the main advantage of using an ad hoc network. Because of this, running an ad hoc network can be more affordable than traditional network because we don't have the added cost of a router.
- **Mobility:**
  The wireless mobile nodes can move at the same time in different directions. Although the routing algorithm can deal with this issue, the performance simulations show that there is a threshold level of node mobility such that protocol operation begins to fail.
- **Speed**
  Creating an ad hoc network from scratch requires a few settings changes and no additional hardware or software. If you need to connect multiple computers quickly and easily, then an ad hoc network is an ideal solution.
- **Fault Tolerance**
  MANET supports connection failures, because routing and transmission protocols are designed to manage these situations.
- **Connectivity**
  The use of centralized points or gateways is not necessary for the communication within the MANET, due to the collaboration between nodes in the task of delivering packets.
- **Fast Installation:**
  The level of flexibility for setting up MANET is high, since they do not require any previous installation or infrastructure and, thus, they cab be brought up and torn down in a very short time.
- **Cost:**
  MANET could be more economical in some cases as they eliminate fixed infrastructure costs and reduce power consumptions at mobile nodes.

VI. LIMITATION OF MANET

- **Bandwidth Constraints:**
  The capacity of the wireless links is always much lower than in wired counterparts. Indeed, several Gbps are available for wired LAN, while, nowadays, the commercial applications for wireless LANs work typically around 2 Mbps.
- **Processing capability:**
  Most of the nodes of the AND are devices without a powerful CPU. Furthermore, the network tasks such as routing and data transmission cannot consume the power resources of the devices, intended to play any other role, such as sensing functions.
- **Energy constraints:**
  The power of the batteries is limited in all the devices, which does not allow infinitive operation time for the nodes. Therefore, energy should not be wasted and that is why some energy conserving algorithms have been implemented (COMPOW,PARO and MBCR are some examples).
- **High Latency:**
  In an energy conserving design nodes are sleeping or idle when they do not have to transmit any data. When the data exchange between two nodes goes through nodes that are sleeping, the delay may be higher if the routing algorithm decides that these nodes have to wake up.
- **Transmission Errors:**
  Attenuation and interferences are other effects of the wireless link that increase the error rate.
- **Security:**
  Analyses some of the vulnerabilities and attacks MANET can suffer. The authors divide the possible attacks in passive ones, when the attacker only attempts to discover valuable information by listening to the routing traffic; and active attacks, which occur when the attacker injects arbitrary packets into the network with some proposal like disabling the network.
- **Location:**
  The addressing is the another problem for the network layer in MANET, since the information about the location the IP addressing used in the fixed networks offers some facilities for routing that cannot be applied in MANET. The way of addressing in MANET has nothing to do with the position of the node.
- **Roaming:**
  The continuous changes in the network connectivity graph involve that the roaming algorithms of the fixed network are not applicable in MANET, because they are based on the existence of guaranteed paths to some destination.
- **Commercially Unavailable:**
  MANET is yet far from being deployed on large-scale commercial basis.

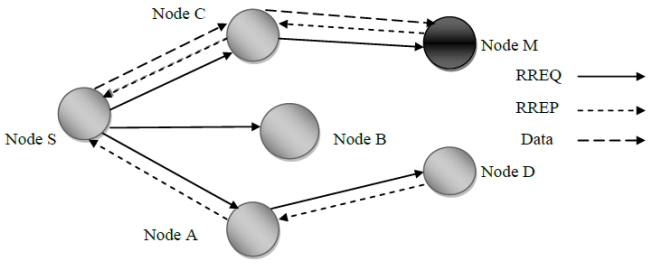

Fig. 2.1 Black Hole Attack

VII. RESEARCH METHODOLOGY

Methodology may be a description of process, or may be explained to include a philosophically coherent of theories, concepts or ideas as they relate to a particular discipline or field of inquiry. It includes the steps that are used for our

research work. The research process carried out includes the following steps:

- Collection of various papers.
- Reading the related literature.
- Identifying the current security problem in MANET.
- Identifying one problem to work out.
- Reading the proposed method (if any) on the identified attack.
- To propose a new algorithm or method to remove identified attack.
- Graphs can be used to show the analysis on various parameters.
- Recommendations based on the analysis.

Floriano De Rango Traditional routing protocols deployed to provide communication among mobile nodes in wireless ad hoc networks (MANET) assume a trust and collaborating environment inside the network. However, this assumption is not always true and a hostile or unprotected environment can seriously affect the protocol and network performance. In this work two kinds of approaches are applied to a well-known routing protocol called SAODV in order to improve its performance and to offer more resilience to attack from malicious nodes authenticated by the network. A preventive approach based on a cryptographic mechanism and reactive approaches to detect the anomalous and malicious behavior of nodes are considered. An extension of SAODV to offer Intrusion Detection mechanism (IDM) and trust based mechanism (TBM) to promote the collaboration of the cooperating node and penalize the selfish nodes are proposed. The extended and proposed protocol SAODV-SDO is presented and simulation results were performed in order to show the effectiveness of our proposal in comparison with AODV and SAODV.

During the route discovery stage, the STAM module of a node switches itself into detecting state when it receives a RREQ (RREP) packet. The purpose of the detection mechanism is to detect attacks and uncooperative behaviors that result indegradation of data transmission. The detection mechanism works in a hop-by-hop style.. An additional purpose of NCP is to defeat possible attack instantiated by adversaries to disrupt the proper functioning of the STAM module. Misbehaving nodes can be detected by detection mechanism and prevented by penalized state. However, there are weaknesses of this solution. That is Packet Processing Time Delay per hop due to the change in state of node time to time, node mobility and congestion.

Vishnu K et al. used the concept of Backbone network. Backbone nodes (BBN) are a group of nodes which are powerful in terms of battery and range. Backbone network is formed with these nodes which are permitted to allocate Restricted IP addresses (RIP) to newly arrived nodes. The author assumes that the environment is in Backbone network. When source node wants to transmit data, it asks the nearest BBN for an unused RIP. Then the source node transmits RREQ to both destination and RIP. If the source node just receives the RREP from the destination, this situation means the network is regular and safe. If the source receives RREP from RIP; however, this situation means there are black hole in this route. Therefore, the source node sends a monitor message to alarm the neighbor node to go into promiscuous mode and let them start to listen the network. The source would send some dummy data packets to destination. At the same time the neighbor node can monitor the situation of the forwarding packets. If the packet loss of the monitored node is beyond the normal case, the neighbor node would alert source node about the situation. The source node would identify the monitored node as black hole by receiving the responded messages of the neighbors. The network environment is assumed that the normal nodes are more than the malicious nodes. The original design of MANETs does not have Backbone network, therefore this concept and method only can suit special environment. If only the RIP method is used, the method cannot lock the black hole and remain need to monitor and observe the suspicious node. Promiscuous mode means that if node A is in the radio transmission coverage of node B, A can overhear packets from B even if the packets are not directly related to A. So a node can listen to every packet sent by its neighbors to realize monitoring operation. This assumption also could be possible, because most current network hardware has the ability to operate the network interface in “promiscuous” mode. This mode enables hardware to deliver every received packet to the network driver software without filtering based on link-layer destination address.

CBDS scheme proposed by Jian-Ming Chang et. al is a malicious node detection scheme, which is able to detect and prevent malicious nodes launching cooperative black hole attacks. It integrates the proactive and reactive defence architectures, and the source node randomly cooperates with a stochastic adjacent node. When source node initializes Route Discovery, it sends out the bait RREQ’ and then source node receives RREP. If RREP is from not existed destination node or intermediate node then trace which node sends back the RREP according to RREP packet’s Record address field. In other words, the black hole is recognized and detected the location of black hole by source node when receiving the fake RREP. Then the detected black hole node is listed in the black hole list and noticed all other nodes to revoke the certificates of black hole by propagating Alarm packets through the network. Further any responses from black hole are discarded. Author assumes that when there is a significant drop in packet delivery ratio, an alarm will be sent by the destination node to the source to trigger the detection mechanism again.

Piyush Agrawal et. al. proposed a complete protocol to detect a chain of cooperating malicious nodes in an ad-hoc network that disrupts transmission of data by feeding wrong routing information. Proposed techniques is based on sending data in terms of equal but small sized blocks instead of sending whole of data in one continuous stream. The flow of traffic is monitored independently at the neighborhoods of both source and destination. The results of monitoring is gathered by a backbone network of trusted nodes. With assumption that a neighborhood of any node in the ad-hoc network has more trusted than malicious nodes, our protocol can not only detect but also remove a chain of cooperating malicious nodes (gray/black hole) by ensuring an end-to-end checking between the transmission of two blocks of data.

Junshan Li et. al. proposed a security architecture is designed based on the artificial immune system by using multi-agents in mobile ad-hoc networks. There are two types of immunity-based agents: At the very beginning, Detection Agent can be regarded as a non-mature T-cell, its behavior patterns are relatively few in the immune memory library. After a period of time, Detection Agent judges its neighbors’ behavior patterns, and retains a part of the aggressive behavior model as

training samples. Behavior patterns in the Immune Memory Library come from two sources, one is training sample from its own Immunity Strategy Library, and the other is behavior patterns in Immune Memory Libraries of other Detection Agents which exchange the patterns regularly in the whole Ad-Hoc network through the Communication Module. Monitor processing module takes charge of monitoring all one-hop neighbors' activities and filtering and encoding them.

Table 3.2: Summary of different proposed solutions

Sr. No.	Proposal Name	Approach	Assumption	Philosophy	Efficiency (PDR)
1.	Dynamic Learning system using DPRAODV	DPRAODV	Multiple Black Hole	Single non-black hole node detects	80-85% under attack
2.	Cooperative black hole node detection using DRI and cross checking	AODV	Cooperative Black Hole	Single non-black hole node detects	60-75%
3.	Black hole node detection using two different solutions	AODV	Single Black Hole	Single node detects	60-75%
4.	Combat with Black hole Attack	MAODV	Single or cooperative	Multiple cooperative non black hole nodes	80-85%
5.	Detecting Black hole Attack on AODV-based Mobile Ad Hoc using dynamic anomaly detection	AODV	Multiple black hole	Single Black Hole node detects	70-80%
6.	Distributed and cooperative mechanism	AODV	Distributed and cooperative	Cooperative detection	High PDR
7.	Prevention of black hole attack using fidelity table	Enhancement on AODV	Multiple Black hole	Multiple non-Black hole node	70-90%
8.	Modified AODV protocol	Modified AODV	Multiple Nodes	Single Source node	Feasible solution

VIII. CONCLUSIONS

After studying the various proposed solutions an assumption have been made which is used in the Table 3.2.

The assumption for Black Hole Attack is categorized as:

1. Single Black Hole Node in a network.
2. Multiple Black hole nodes in the ad hoc network.

It simplifies that whether there is single node that acts as Black Hole or multiple Black Hole nodes act as malicious nodes in cooperative nature to grab the packets.

The philosophy for the Black Hole Attack detection proposals can be categorized as below:

1. Single non malicious node identifying a black hole node
2. Multiple non malicious nodes identifying a black hole node.

REFERENCES

[1] Poongothai T. and Jayarajan K., "A non cooperative game approach for intrusion detection in Mobile Adhoc networks", Internatonal conference of computing, communication and networking (ICCC), 18-20 Dec 2008, St. Thomas, VI, pp 1-4.

[2] DjamelDjenouri and LyesKhelladi, "A survey of security issues in mobile ad hoc and sensor network", IEEE communications Surveys and Tutorials journal,Volume 7, Number 4, 2005, pp 2-29.

[3] Michele Nogueria Lima, AldriLuiz dos Santos and Guy pujolle, "A Survey of Survivability in Mobile Ad Hoc Networks", IEEE Communications Surveys and Tutorials COMSUR), Volume 11, Number 1, 2009, pp 1-3.

[4] NishuGarg and R.P Mahapatra, "MANET Security Issues", International journal of Computer Science and Network Security (IJCSNS), Volume 9, Number 8, 2009, pp. 241-246.

[5] Wenjia Li and Anupamjoshi, "Security Issues in Mobile Ad hoc Networks – A Survey". Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore Country, 2006.

[6] Bing Wu, Jianmin Chen, Jie Wu and MihaelaCardei, "A Survey on Attacks and countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network security, ch-12,2006.

[7] Hao yang, Haiyunlyo, Fan Ye,Songwu Lu and Lixi

[8] HesiriWeerasinghe "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, Volume 2, 2007, pp 362-367.

[8] Mehdi Medadian, M.H. Yektaie and A.M.Rahmani, " Combat with Black Hole Attack in AODV routing protocol in MANET", First Asian Himalayas International Conference on Internet (AH-IC12009), 3-5th Nov, 2009.

[9] Bo sung Yong, Guan Jianchen and Udo W. Pooch, " Detecting Black-hole Attack in Mobile Ad hoc Networks", The Institution of Electrical Engineers (IEE), Volume 5, Number 6, 2003, pp 490-495.

[10] ElmarGerhards- Padilla, Nils Aschenbruck, Peter Martini Marko Jahnke and Jens Tolle, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", 32nd IEEE Conference on Local Computer Networks, 15-18th Oct 2007, Dublin, pp 1043-1050.

[11] GaoXiaopeng and Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", IFIP International Conference on Network and Parallel Computing – Workshops, 18-21 Sep 2007, Dalian, China, pp 449-460, 2009.