International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-4 Issue-3, August 2014

Evaluation and Analysis of Wireless Networks & MANETS

Kirna Rani, Kamaljeet Kaur Magnat

Abstract*— A network is a collection of two or more computer systems which connected with each other. It is type of replace of information to communicate with one another. It is an association or set up of computer devices which are involved with the communication facilities. When number of computer is connected simultaneously to exchange information they form networks and contribute to resources. Networking is used to distribute information like data communication. Sharing resources can be software type or hardware types. It is central administration system or supports these types of system [1]. The communications protocols used to organize network traffic, with the network's size, its topology and its organizational intent. A network can be wired network and wireless network. Wired network is that which used wires for communicate with each other's and wireless network is that which communicate without the use of wires through a medium. In order to detect and Isolation of Selective Packet Drop Attack in Mobile Ad hoc Networks, we will discuss how study and evaluate the Selective packet Drop attack in MANET and its consequences in this paper.

***Index Terms*—Wireless Sensor Network, MANET, AODV.**

I. INTRODUCTION

A network is a group of two or more computer systems which linked together. It is mode of exchange of information to communicate with one another. It is a connection of computer devices which are attached with the communication facilities [1]. When number of computer are joined together to exchange information they form networks and share resources. Networking is used to share information like data communication. Sharing resources can be software type or hardware types. It is central administration system or supports these types of system.

Different types of networks are as following:

- Transmission media based networks like wired network and wireless network.
- Network Size based network like MAN, LAN and WAN.
- Management based networks like peer-to-peer and client/server.
- Topology based networks called connectivity like bus, star, and ring topology.

A network can be wired network and wireless network. Wired network is that which used wires for communicate with each other's and wireless network is that which communicate without the use of wires through a medium.

Manuscript published on 30 August 2014.
*Correspondence Author(s)
Kirna Rani, M.Tech, Department of Computer Science and Engineering,Punjabi University Regional Center for Information Technology and Management, Mohali, Punjab, India.
Kamaljeet Kaur Magnat, Asst. Prof., Department of Computer Science and Engineering, Punjabi University Regional Center for Information Technology and Management, Mohali, Punjab, India.

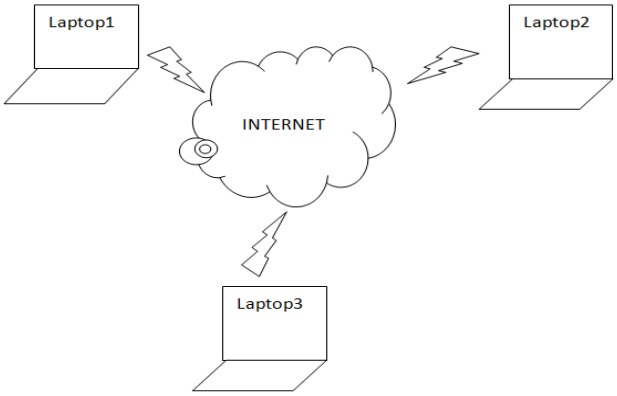

Fig. 1 Diagram of Computer Networks

II. BACKGROUND

The use of the wireless sensor network grow in every field. The main field in which the wireless sensor network used are ,in military battlefield ,in commercial sector, personal area network local level, industrial process monitoring ,in agriculture for monitoring the temperature, sunlight etc. Even the wireless sensor network is more popular but it faces many challenges like security, power consumption multicasting bandwidth and storage capacity. The most challenging issue in wireless sensor network is security. Various methods like defensive mechanism scheme, key distribution, multipath forwarding technique, elliptic curve technique etc, are already used to solve this problem, but every method has some drawback. In this Thesis we use a new technique to solve the security problem and compare it with the existing work.

- To study and evaluate the selective packet drop attack in MANET and its consequences.
- To detect the selective packet drop in MANET using AODV protocol.
- To propose a new scheme to detect malicious node in the network which are responsible for triggering the selective packet drop attack in the network.
- Simulating the detection of selective packet drop attack using AODV protocol in MANET using NS-2 tool.

Firstly we deploy the mobile ad hoc network with infinite number of mobile nodes. All the mobile nodes are randomly deployed into the fixed area. The source and destination are selected for route establishment. For the route establishment source node flood the route request packet in the network and route reply packets are send back to the source by the adjacent nodes. The route is established between source and destination on the basis of hop counts and sequence numbers.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The malicious node exists in the route which is selected between source and destination. The malicious node will be responsible for triggering the selective packet drop attack. The proposed methodology will detect the malicious node and isolate, it from the network. In Delay sensitive selective packet drop attack in which either packets drop or transfer to other route to reach to the destination by malicious node. In throughput sensitive packet dropped by the malicious node. In our proposed work we overcome the problem of dropped packet by detecting them and redirect to the source with the help of monitoring nodes.

- We will enhancement in AODV Protocol to detecting the selective packet drop.
- We use the monitor mode algorithm to detect and isolate the malicious node in the network.
- After that we implement the AODV protocol on NS2 simulator for acquire the result.
- The proposed methodology will be implemented in network simulator version 2.

III. Wireless Sensor Network

Wireless Networks term is refers to a kind of networking that do not requires cables to connect with devices during communication. The transmission is take place with the help of radio waves at physical level [2]. It is also known as Wi-Fi or WLAN. With the help of this network, devices can be joined easily with the help of radio frequency without wires to sharing information. The IEEE standard for wireless network is 802.11. Wireless Networking is a technology in which two or more computers communicate with each other using standard network protocols and without the using of cables [3].

There are two types of Wireless Operating modes:

- Infrastructure Mode:- In infrastructure based network, communication is takes place only between the wireless nodes and the access points. The communication is not directly takes place between the wireless nodes. Here the access point is used to control the medium access as well as it acts as the bridge to the wireless and wired networks. In this network, fixed base stations are used when the node goes out of the range of base station another base station come into range. The example of infrastructure based network is cellular networks. It is centralized system which is controlled by the controller like router [1]. The main problem in this system is that if controller fails all the system will crash.

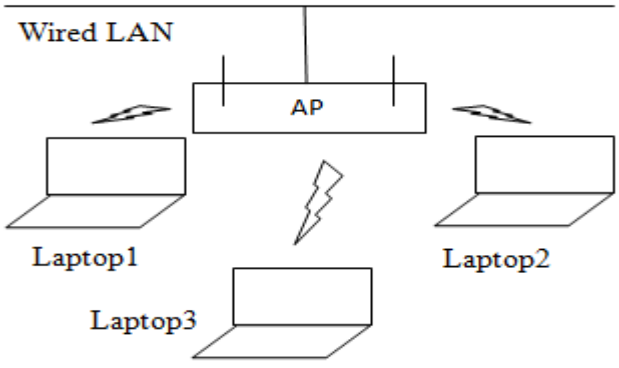

Fig. 2 Infrastructure Mode

- Ad hoc Mode or Infrastructure less Mode:- The infrastructure less network does not need any infrastructure to work. In this network each node can communicate directly with other nodes. So in this network no access point is required for controlling medium access. Infrastructure less networks do not have routers that are fixed. In this network all the nodes need to act as routers and all nodes are capable of movement and can be connected dynamically in an arbitrary manner. All the devices in infrastructure less network are wirelessly communicated to each other. In infrastructure less network file server contain base station of Wi-Max which controls all access points the range of 6kms.Using Wi-Max base station and access points communicating and using Wi-Fi user and access points communicating [5]. Here Figure shows a simple peer to peer network with three nodes. The outermost node is outside of transmitter range of each other. To forward packets between the outermost nodes, the middle node can be used. Three nodes have formed an ad-hoc network middle node is behave like a router [1]. It is of three types. The subcategories are given below:
  - Wireless Sensor Networks
  - Manet
  - Wireless Mesh Network

IV. Adhoc Wireless Sensor Network

Ad hoc network is a decentralized type of wireless network. There is no pre-existing infrastructure such as routers in wired networks or access points in wireless networks on which it is depended. In routing each node participates by forwarding data for other nodes in ad hoc network the determination of which nodes forward data is made dynamically on the basis of network connectivity. Ad-hoc networks are a new standard of wireless communication for mobile hosts. Basically it's a network which is used in urgent situation causes. No fixed infrastructure in ad hoc network like base stations is required. Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. Wireless networks refer to those networks that make use of radio waves or microwaves in order to establish communication between the devices. All the nodes act as router in ad hoc network. The wireless network offers certain advantages over the wired networks that are as follows [2]

- It is very easy and fast to set up a wireless system and it eliminates the need for wires and cables.
- Wireless networks can be extended to the places that cannot be wired.
- It adapt easily and more flexibility to changes in the configuration of the network.

There are two types of classification available in ad hoc networks which are as following:

- Single-hop:- In this hop nodes are in direct communication and both nodes are in range of each others. The chances of link failure are more in this hop.
- Multi-hop:- In this hop nodes are communicate with the help of internal nodes not directly. To reach from source to destination internal nodes participate.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

There different types of ad hoc network available. These are as following:

• MANET:- MANET stands for Mobile Ad hoc Network. It is a robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly connected with each other and forming arbitrary topology. They can act as both routers and hosts. They have ability to self-configure makes this technology suitable for provisioning communication to, for example, disaster-hit areas where there is no communication infrastructure or in emergency search and rescue operations where a network connection is urgently required. In MANET routing protocols for both static and dynamic topology are used. An ad hoc network is a wireless network describe by the nonexistence of a centralized and fixed infrastructure. The absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks. Therefore, we refer to a wireless ad hoc network with mobile nodes as a Mobile Ad Hoc Network. In a MANET, mobile nodes have the capability to accept and route traffic from their intermediate nodes towards the destination, i.e., they can act as both routers and hosts. More frequent connection tearing and re-associations place an energy constraint on the mobile nodes.

- AODV (Ad hoc on Demand Distance vector)
- DSR (Dynamic Source Routing)
- OLSR (Optimized Link State Router)
- Wireless Routing Protocol (WRP)
- Zone Routing Protocol (ZRP)
- In MANETs, collection of mobile nodes may dynamically vary the topological structure. With respect to the more widely used mobile cellular networks .Mobile Ad Hoc Networks do not use any form of fixed infrastructure or centralized administration. These types of networks have the salient characteristics: dynamic topologies, bandwidth constraints, variable capacity links, limited physical security and energy –constrained operations [7].

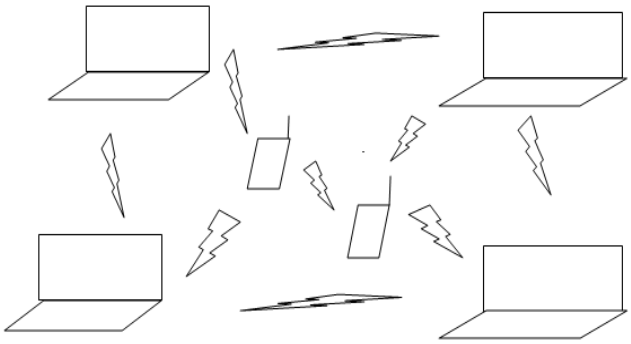

Fig. 3 Diagram of MANET

- Wireless Sensor Networks (WSN)
- Wireless Mesh Networks (WMN)

V. ATTACKS ON MANET [8]

• **Passive Attacks:**
A passive attack obtains data exchanged in the network without disturbing the communications operation. The passive attacks are difficult to detection [4]. In its, operations are not affected [8]. The operations supposed to be accomplished by a malicious node ignored and attempting to recover valuable data during listens to the channel [10]. Examples of Passive Attacks are eavesdropping, snooping.

• **Active Attacks:**
An active attack is that attack which any data or information is inserted into the network so that information and operation may harm [4]. It involves modification, fabrication and disruption and affects the operation of the network [10].

• **Internal Attack:**
Internal attacks are as of compromised nodes that are part of the set of connections. In an internal attack from the network the malicious node gains unauthorized access and behave as a genuine node. Traffic can be analyze between other nodes and may participate in the activities of other networks [6].

• **External Attack:**
The external attack is conceded out by the nodes which do not belong to network. It may cause unavailibity and congestion by sending false information for the network [12].

• **Denial of Service Attack:**
The main purpose of this attack is to attack the entire network. In this type of attack the attacker mainly uses the radio signal jamming and exhaustion method [18].

• **Eavesdropping:**
Eavesdropping is a passive attack. In this type of attack the nodes acquire the confidential information. After that this confidential information is used by the malicious node. This mystery information like private key public key password can be draw by the eavesdropper [18].

• **Wormhole Attack:**
In this type of attacks an attacker receives data at one point in the network and put it to the other point in the network, and after that replays them into the network from that point [18].

• **Replay Attack:**
Replay attack is a attack in which attacker that perform replay attack and retransmit the valid data frequently to introduce the network routing traffic that curb the existing. The main aim of this type of attack is an attack on the new route. It can be used for damage the security solution [18].

• **Jamming:**
In this type of attack the attacker firstly keep the accessing wireless medium in order to calculate the frequency at which the destination node is receiving the signal from the sender. After that it transmits the signal on that frequency [18].

• **Man-in-the Middle Attack :**
In this type of attack the attacker lie between the sender and receiver and gains the information sent between two nodes. In many situations, attacker pretends the sender to communicate with the receiver or pretend the receiver to replay to the sender [18].

• **Gray-Hole Attack:**
It is also called as routing misbehavior attack which leads to dropping of messages. This attack is classified into two parts. In the first part the node promote itself as hold a valid route to destination, in the second part nodes drops intercepted packet with a specific probability [18].

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

VI. Characteristics of WSN

ADVANTAGES: - The main advantages of the Ad hoc networks are as follows:

- It is decentralized system that can be setup at anywhere. There is no need of central controller and provide mobility.
- MANET works without the help of pre-existing networks.
- It provides services and access to the data at the geographical position.
- It can be easily scalable by adding more devices which are movable in nature.
- It can be act as a router and hosts also.

DISADVANTAGES:- The disadvantages of MANET are as following:

- It has limited resources.
- It has lack of authorization services.
- Topology changes frequently.
- The protocols which are used in wired networks cannot be used in ad hoc networks.
- It is difficult to detect malicious node due to change of topology.

APPLICATIONS:-

- Emergency Services
- Military Battlefield
- Entertainment and Local level
- Commercial Environments
- Personal Area Network (PAN)

ISSUES/PROBLEMS:-

- **Routing:** The efficient routing protocols are necessary to set up the communication path between the nodes, without causing desirable control traffic overhead[21].Most of the protocols should be based on the reactive routing protocols on the place of proactive routing protocols. Routes between the nodes hold multiple hops, which is very complicated than the signal hop communication [18].
- **Security and Reliability:** The features of distributed operation need different method of authentication and key management [18].
- **Quality of Service:** The derived features of communication quality in a MANET make it difficult to provide a fixed guarantee on the action offered to a device.
- **Multicast:** The multicast routing protocols must be able to deals with mobility included multicast membership dynamics [18].

VII. Routing Protocol

Routing protocol specifies how to communicate with the help of routers. It shares information among intermediate nodes then with the whole network. It helps to search shortest route from source to destination [15]. There are mainly two types of routing protocol available. These are as following:

- **Proactive Routing Protocol:**

In protocol one node contains more than one table for each node in the network. All the nodes are update regularly. If the topology frequently changes than update information propagate to every node of the network and update table.

- **Reactive Routing Protocol**

It is on-demand protocol. It is lazy approach in which all the node are not contains the information of the all the nodes and maintains table only on demand. To find the path route discovery process is follow. Reactive routing protocols are bandwidth efficient. In this, routes are built as and when they are required. This is achieved by sending route requests across the network. There are disadvantages with this protocol that it offers high latency when finding routes and other is the possibility of network clog when flooding is excessive. In this thesis, we considered AODV, DSR and DSDV [6].

VIII. Ad-Hoc On-Demand Distance Vector

AODV is an on-demand routing protocol used in ad hoc networks. This protocol is like any other on-demand routing protocol which facilitates a smooth adaptation to changes in the link conditions. In case when a link fails, messages are sent only to the affected nodes. With this information, it enables the affected nodes invalidate all the routes through the failed link. AODV has low memory overhead, builds unicast routes from source to the destination and network utilization is less. There is least routing traffic in the network since routes are built on demand. When two nodes are in an ad hoc network wish to establish a connection between each other, it will enable them build multihop routes between the mobile nodes involved. It is loop free protocol which uses Destination Sequence Numbers (DSN) to avoid counting to infinity. This one is the distinguishing feature of this protocol. Requesting nodes in a network send Destination Sequence Numbers (DSNs) together with all routing information to the destination. It selects the optimal route based on the sequence number [7]. AODV defines three messages: Route Requests (RREQs), Route Errors (RERRs) and Route Replies (RREPs). These messages are used to discover and maintain routes across the network from source to destination by use of UDP packets. Whenever there is need to create a new route to the destination, the node which is requesting broadcasts Route Requests. A Route is determined when this message reaches the next hop node (intermediate node with routing. Information to the destination) or the destination itself and the RREP has reached the originator of the request. Routes from the originator of the RREQ to all the nodes that receive this message are cached in these nodes. When a link failure occurs, Route Errors (RERRs) message is generated [7].

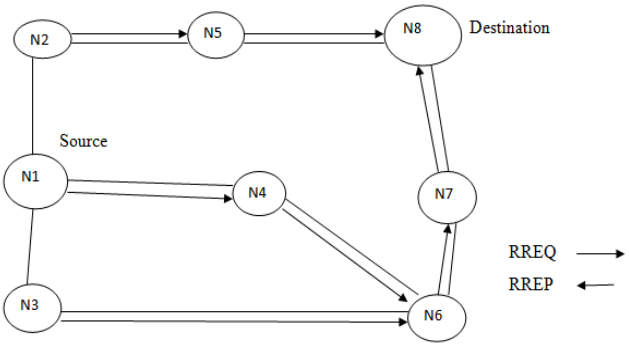

Fig. 4 AODV Algorithm

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

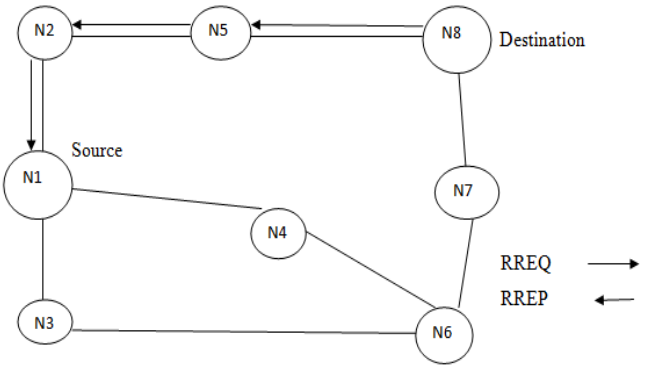

Fig. 5 Best Path with Minimum Hop Count

In the figure 5 N1 nodes broadcasts the packets to its neighbor nodes with RREQ and update its table. Then these nodes further forwards packets to its neighbor until the destination find outs and fresh route find out. Each node maintains its sequence number and broadcast ID. For every RREQ the node initiates broadcast ID which is incremented and together with the node's IP address uniquely identifies an RREQ. At last that route will be the final route that has the minimum hop count from source to destination.

DSR: It is a reactive routing protocol for ad hoc wireless networks. It also has on-demand features like AODV but it's not table-driven. It is based on source routing. The Dynamic Source Routing protocol (DSR) is a simple designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes and efficient routing protocol. DSR allows the network to be fully self-organizing and self-configuring.

IX. SELECTIVE PACKET DROP

Selective Packet drop attack is the type of denial of service attack. Packet dropping attack is launched on the forward phase. So it is very complex and difficult to isolate. This attack is very easy to perform but very difficult to detect it. Selfish node also drop packet in their different ways. They drop packets only to save their resources not damage any other nodes. Selective forwarding attacks may damage some mission of applications. In these types of attacks, malicious nodes act as normal nodes every time but selectively drop sensitive packets, such as packet coverage the movement of the differing forces. Such selective dropping is tough to detect. Counter measures to selective forwarding attacks cannot recognize malicious nodes or need time synchronization. Selective forwarding attacks can root serious threats on many applications. Selective forwarding attacks have some nodes which drop some or all packets. Attacker can initiate the selective forwarding attack and crash a portion of packets for which it require to store set while forward the rest. Selective forwarding attack is complex attack to detect, since packet drops in sensor networks may be caused by untrustworthy wireless communications or node failures. Selective Packet drop is only possible when jamming attack is unsuccessful. Once the packet is expected by the compromised node, it can examine the packet headers, categorize the packet, and decide whether to forward it or not. This action is known as misbehavior. Post-reception dropping is fewer bendy than selective jamming because the challenger is limited to dropping only the packets routed through it. Selective policy known as the Jellyfish attack which is a compromised node that is occasionally drops a small part of consecutive packets and can be efficiently reducing the throughput of a TCP flow to near zero. This attack can be achieve even by remind random delays to TCP packets, without dropping them, while left over protocol compliant. Similar selective dropping attacks can be construct for other network functions such as the association/de-association of STAs, and topology management [lazos].

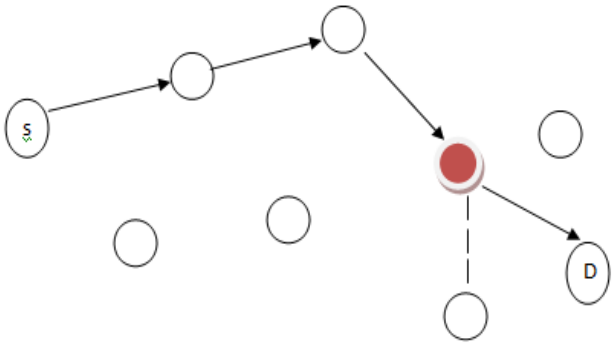

Fig. 6 Diagram of Packet Drop

Migration of Selective Dropping:

Selective dropping attacks can be mitigated by employing fault-tolerant mechanisms at a variety of layers of the protocol stack. At the routing layer, multi-path routing provides tough multi-hop communication in the occurrence of association faults, by utilizing more than one path from a source to a destination. A selective dropper can always feature his losses to congestion, in order to avoid detection as a malicious node. In this case, classification mechanisms employing long-term statistics, can accurately pinpoint selective droppers.

Identification of Selective Droppers:

- Reputation Based System

This system identifies misbehaving nodes based on per-node reputation metrics, computed based on interactions of each node with its peers. These systems typically incorporate two critical operations. These operations are as follow:

(a) The collection of accurate observations of nodes' behavior

(b) The computation of the reputation metric.

- ACK based System

In ACK-based scheme which is differ from overhearing techniques in the method of collecting first-hand behavioral observations. Downstream nodes are dependable for acknowledging the reception of messages to nodes several hops upstream. These systems are appropriate for monitoring the exact relay of unicast traffic, at the expense of communication overhead for relaying a supplementary set of ACKs. ACK-based schemes cannot be used to recognize insiders with the purpose of selectively fall broadcast packets. Such packets stay, in general, unacknowledged in wireless networks, to keep away from an ACK implosion situation. Moreover, a small set of colluding nodes can still offer real ACKs to upstream nodes while dropping packets.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- Credit Based System

In Credit-based systems alleviate selfish behavior by incentivizing nodes to forward packets. Nodes that relay traffic obtain credit in return, which can be later used up to promote their own traffic. However, in the context of WNMs, MPs do not produce any traffic of their own, but act as dedicated relays. Hence, compromised MPs have no incentive for collecting credit. Furthermore, in the case of selective dropping attacks, misbehaving nodes can at rest collect sufficient credit by forwarding packets of low importance, while dropping a few packets of "high value." In addition, the credit collected by a particular node depends.

X. LITERATURE ASSOCIATED

The selective packet drop attacks and AODV protocols are used to solve the objective. In this paper we present the survey on AODV, which is mainly used for route establishment in the network. Various research papers reviewed based on this technique:

Steven M. Bellovin and Michael Merritt, discussed about Kerberos authentication protocol and various limitations of Kerberos authentication protocol [9]. The main limitation of Kerberos authentication protocol is much number of message exchange is needed for successful authentication and this approach will degrade the battery performance of the hand held devices. Second, disadvantage is the assumptions of the Kerberos authentication protocol when environment changes assumptions are need to change for efficient working of Kerberos protocol. Reply attack, login spoofing, session key expose, password guessing attacks are possible in Kerberos authentication protocol.

Seung Yi and Robin Kravets had discussed various mutual authentication schemes of mobile ad hoc network. They had discussed the symmetric key and asymmetric key distribution schemes [10]. They had also discussed PKI (public key distribution) scheme which based on the symmetric key distribution scheme. In this paper author proposed a new authentication scheme named as MOCA which hybrid type of scheme and use both PKI and asymmetric schemes for mutual authentication.

Pradeep Kyasanur et.al proposed a protocol extension of 802.11 DCF protocol to detect the selfish behavior of the nodes in the infrastructure and ad hoc network topologies. Selfish nodes means the nodes which select the conventional window (CW) time in such a way so that the other nodes are keep on waiting to send the data and overall through put of the network degrade [11]. The proposed scheme has three components first one is that the receiver decides that whether sender is diverting form protocol or not. Second component is penalize ,in this scheme the receiver assigns the conventional window time to the sender if sender not sends data in that time period sender have to pay the plenty. Plenty means that in next time when sender sends that data they have to wait more to send data to receiver .The third component is the diagnosis scheme receiver decide whether the sender is selfish or not on the basis of the total data send by the sender and number of times the sender pay plenty .if no of plenty paid by the sender is more than the threshold value which is fixed then the sender is selfish and no more data is received form that sender.

Yixin Jiangand et.al In this paper they have proposed a new mutual authentication and key exchange protocol. The two main features of this protocol is identity anonymity and session key renewal. This protocol provides secure roaming services to the legitimate user between the home and visiting agent or in short, this protocol provides secure handoff to the legitimate user [12]. The proposed protocol is based on the secrete splitting principle and self-certified scheme. The protocol works in two phases: First phase is the mutual authentication with anonymity which hides the use's real identity when a legitimate user is roaming from the home agent to the visiting agent. This phase use the temporal identity (TID) instead of the user's real identity. Second phase is the session key renewal phase which renews the shared key which is shared between the legitimate user and the serving agent.

Caimu Tang et.al proposed efficient authentication mechanisms for low-power devices. In the proposed scheme the mobile station only need to pass one packet for mutual authentication .They used the elliptic-curve-crypto system based trust delegation Mechanism to generated group pass code for mobile station authentication [13]. With the use of this authentication mechanism many active and passive attacks will be prevented including the denial of service attack. The mobile device authenticated with the visiting base station only by the exchange of one packet .This purposed mechanism is required less computations and less message exchange as compared to other authentication schemes.

Tien-Ho Chen and Wei-Kuan Shih had discussed about importance of mutual authentication for wireless sensor networks .They also discussed about the DES protocol which is the hash-based authentication protocol[14] ,this protocol provides the security against the stolen-verifier, masquerade, replay, and guessing attacks. In this paper they had also discussed about the weakness of the das protocol, they had proposed an certain enhancements in the das protocol .The enhanced das protocol is efficient than the traditional das protocol .Enhanced das protocol is reliable protocol and provides more security to the sensor nodes in the insecure environment. The proposed protocol is the energy efficient protocol and require less message exchange and less computations for mutual authentication.

Sushma Yalamanchi and K.V. Sambasiva Rao, they had proposed a two stage authentication scheme for wireless networks. They discus that in wired network use the authentication protocol which is having large computations but in wireless networks we require less computation and energy efficient authentication protocol .Because in wireless networks the hand held devices are having limited battery and limited computational resources also wireless networks on suffer from packet losses and bit errors and offers low bandwidth [15]. In the paper, they presents a two-stage authentication scheme for wireless networks that uses a computationally intensive but highly secure strong authentication in Stage 1 and a lightweight symmetric key based protocol in Stage 2.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The cost of the strong authentication adopted in Stage 1 is amortized over N sessions thus reducing the overall cost of the scheme. We adapt the Dual-signature based IKE authentication that we proposed in our earlier work and employ it as Stage 1 authentication. The Symmetric key protocol in Stage 2 authentication that we propose uses the symmetric keys that are generated in Stage 1.

Jacek Cicho et.al discussed the problem of efficient alarm protocol for ad-hoc radio networks consisting of devices that try to gain access for transmission through a shared radio communication channel [16]. The problem arises in tasks that sensors have to quickly inform the target user about an alert situation such as presence of dangerous radiation, fire, seismic vibrations, and more. In this paper, we show a protocol which uses O (log n) time slots and show that (log n= log n) is a lower bound for used time slots.

S. Sharmila and G. Umamaheswari discussed about the defensive mechanisms based on cumulative acknowledgement and energy based is proposed to detect selective forward attack in mobile wireless sensor networks . The scheme is evaluated in terms of packet delivery ratio and throughput. The malicious node is detected based on the acknowledgement and energy level of the node [17]. The energy consumption of the detection scheme is less when compared with existing detection schemes. From the simulations, byte overhead is 0.39 percentages and detection accuracy is 80% are observed and thus increasing the network throughput. These results show that the packets can be forwarded without any selective packet drop by minimizing the malicious nodes in the network. The further enhancement of the proposed scheme is to improve the success rate to 100% with various mobility and receiver sensitivity of the node.

Priyanka Goyal et.al discussed about the Mobile ad-hoc network is one of the most promising fields for research and development of wireless network [18]. As the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. Due to brutal challenges, the special features of MANET bring this technology great opportunistic together. This paper describes the essential problems of ad hoc network by including the idea, features, category, and vulnerabilities of MANET. This paper presents an overview and the study of the routing protocols. Also include the several challenging issues, emerging application and the future trends of MANET.

Donatas Sumyla, author discussed about the history of Manet and its difference with ad hoc networks, its origin and its need and importance. He also introduced in this paper about the routing protocols of Manet which are widely used for the transferred of data from source to destination [19]. Table driven routing protocols, source-initialized routing protocols their sub-categories are mentioned in this paper.

Amandeep Singh Bhatia and Rupinder Kaur mentioned about the wireless networks are increasing in popularity with current advances in technology, the architecture of such networks is not based on a centralized base station but on each node which acts as a router and forwards data packets to other nodes in the network. The technologies have driven into new era with the introduction of ad hoc networks and the concept behind the ad hoc networks is it works without the access points [20]. It has features like adaptive, self organizing and decentralized in nature. Due to these specialized features, it has become a popular technology. So, there has been an inevitable need of a good routing protocol in order to establish the connection between the nodes since the mobile nodes can change their topology frequently. The movement of the mobile node is one of the important characteristics because it can affect the performance of the ad hoc network protocol. This paper has analyzed the mobility of the random waypoint model for different routing protocols in mobile ad-hoc network. Once the route has been established, the performance of AODV protocol shows better results throughout the simulation time except beginning and ending time. The On-demand protocols, DSR and AODV performed particularly well with increased in number of loads, the window size evolution of AODV is very well.

Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester In the past few years, we have seen a rapid expansion in the field of mobile computing due to the proliferation of inexpensive, widely available wireless devices [21]. However, current devices, applications and protocols are solely focused on cellular or wireless local area networks (WLANs), not taking into account the great potential offered by mobile ad hoc networking. A mobile ad hoc network is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure. This type of network, operating as a stand-alone network or with one or multiple points of attachment to cellular networks or the Internet, paves the way for numerous new and exciting applications. Application scenarios include, but are not limited to: emergency and rescue operations, conference or campus settings, car networks, personal networking, etc. This paper provides insight into the potential applications of ad hoc networks and discusses the technological challenges that protocol designers and network developers are faced with. These challenges include routing, service and resource discovery, Internet connectivity, billing and security.

Loukas Lazos and Marwan Krunz discussed about WMNs are prone to various external and internal security threats. While most external attacks can be mitigated with a combination of cryptographic mechanisms and robust communication techniques, internal attacks are much harder to counter because the adversary is aware of the network secrets and its protocols. Jamming resistant broadcast communications in the presence of inside jammers remains a challenging problem. Current solutions attempt to eliminate the use of common secrets for protecting broadcast communications. Such secrets can be easily exposed in the event of node compromise. However, the heightened level of security comes at the expense of performance, because broadcasted messages have to be transmitted multiple times and on multiple frequency bands to guarantee robust reception.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Moreover, even if packet reception of critical messages is ensured, inside adversaries are in complete control of the traffic routed through them. A large body of literature addresses the problem of misbehavior in the form of packet dropping by developing reputation systems, credit-based systems, and communication-intensive acknowledgment schemes. Despite the relative wealth of literature on this problem, significant challenges are yet to be addressed. Most existing methods assume a continuously active adversary that systematically drops packets. These adversaries are detected by aggregate behavioral metrics such as per-packet reputation and credit. However, these metrics cannot detect attacks of selective nature, where only a small fraction of "high value" packets is targeted. Furthermore [22], when the adversary drops only a few packets, his behavior can be indistinguishable from dropping patterns due to congestion or poor wireless conditions. Further challenges include efficient behavioral monitoring mechanisms not relying on continuous overhearing and efficient maintenance a dissemination of reputation metrics.

Jiazi YI author examined the applications of MANET nowadays. The report not only reviews the pure general-purpose MANET, but also other specified MANETs: mesh networks, opportunistic networks, vehicular ad hoc networks and wireless networks [23]. We can see that, although pure general-purpose MANET does not yet exist in the real world, the multihop ad hoc networking paradigm was successfully applied in several classes of networks that are penetrating the mass market.

Ian D. Chakras and Elizabeth M. Belding-Royer analyzed the design possibilities for an AODV implementation. They first identified the unsupported events needed for AODV to perform routing. One of the most motivating reasons to use simulation is the difficulty of creating a real implementation. In a simulator, the code is contained within a single logical component, which is clearly defined and accessible. On the other hand, creating an implementation requires use of a system with many components, including many that have little or no documentation. The implementation developer must understand not only the routing protocol, but all the system components and their complex interactions. Further, since ad hoc routing protocols are significantly different from traditional routing protocols, a new set of features must be introduced to support the routing protocol. In this paper we describe the event triggers required for AODV operation, the design possibilities and the decisions for our Ad hoc On-demand Distance Vector (AODV) routing protocol implementation, AODV-UCSB. This paper is meant to aid researchers in developing their own on-demand ad hoc routing protocols and assist users in determining the implementation design that best of their needs. They then examined the advantages and disadvantages of three strategies for determining this information. This analysis supported our decision to use small kernel modules with a user-space daemon. Finally, they presented the design of many publicly available AODV implementations. They hope that the information in this paper aids researchers in understanding the trade-offs in ad hoc routing protocol implementation development [24]. Further, the description of the design structure and additional features of each implementation can assist users in deciding which implementation best of it's their needs.

REFERENCES

1. Sunil Taneja, Dr. Ashwani Kush, Amandeep Makkar, "End to End Delay Analysis of Prominent On-demand Routing Protocols", IJCST Vol. 2, Issue1, March 2011
2. ABDUL HAIMID BASHIR MOHAMED, thesis, "ANALYSIS AND SIMULATION OF WIRELESS AD-HOC NETWORK ROUTING PROTOCOLS"2004
3. Giovanni Vigna Sumit Gwalani Kavitha Srinivasan Elizabeth M. Belding-Royer Richard A. Kemmerer, "An Intrusion Detection Tool forAODV-based Ad hocWireless Networks", 2004
4. Sevil Şen, John A. Clark, Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks", 2010
5. Rusha Nandy, "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme" Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043 (2011)
6. Wenjia Li and Anupam Joshi , "Security Issues in Mobile Ad Hoc Networks- A Survey",2005
7. Gene Tsudik, "Anonymous Location-Aided Routing Protocols for Suspicious MANETs", 2010
8. Karim El Defrawy, and Gene Tsudik , "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs" , IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 9, SEPTEMBER 2011
9. Steven M. Bellovin and Michael Merritt "Limitations of the Kerberos Authentication", USENIX – winter 1991
10. Seung Yi, Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks" , 10 th IEEE International Conference on Network Protocols (ICNP'02) 1092-1648
11. Pradeep kyasanur "Selfish MAC layer Misbehavior in wireless networks", IEEE on Mobile Computing, 2005
12. Yixin Jiang Chuang Lin, Minghui Shi, Xuemin Shen "Multiple Key Sharing and Distribution Scheme With (n; t) Threshold for NEMO Group Communications", IEEE 2006
13. Caimu Tang ,Dapeng Oilver "An Efficient Mobile Authentication Scheme for Wireless Networks", IEEE
14. Tien-Ho Chen and Wei-Kuan, Shih, "A Robust Mutual Authentication Protocol for Wireless Sensor Networks ETRI Journal, Volume 32, Number 5, October 2010
15. Sushma Yalamanchi and K.V. Sambasiva Rao "Two-Stage Authentication For Wireless Networks Using Dual Signature And Symmetric Key Protocol" International Journal of Computer Science and Communication (IJCSC), n Vol. 2, No. 2, July-December 2011, pp. 419-422
16. Jacek Cicho, Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada "On Alarm Protocol in Wireless Sensor Networks", 2010
17. S. Sharmila and G. Umamaheswari, " Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks", *International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012*
18. Priyanka Goyal, Vintra Parmar and Rahul Rishi , " MANET: Vulnerabilities, Challenges, Attacks, Application" , *IJCEM International Journal of Computational Engineering & Management*, Vol. 11, January 2011 ISSN (Online): 2230-7893 2011
19. Donatas Sumyla, **"** Mobile Adhoc Networks**" ,** IEEE Personal Communications Magazine, April 2003, pp. 46-55.
20. Amandeep Singh Bhatia and Rupinder Kaur Cheema ,"Analysing and Implementing the Mobility over MANETS using Random Way Point Model" , International Journal of Computer Applications (0975 – 8887) Volume 68– No.17, April 2013
21. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester , " An overview of Mobile Adhoc Networks: Applications and challenges", Sint Pietersnieuwstraat 41, B-9000 Ghent, Belgium ,2005

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

22. Loukas Lazos, and Marwan Krunz, "Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks" Dept. of Electrical and Computer Engineering, University ofArizona, Tucson, Arizona, 2009
23. Jiazi YI , " A Survey on the Application of MANET", 2005
24. Ian D. Chakeres and Elizabeth M. Belding-Royer , "AODV Routing Protocol Implementation Design", In C. E. Perkins, editor, Ad hoc Networking, pages 173.219. Addison-Wesley, 2004
25. Rusha Nandy, "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme" Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages: 1035-1043 (2011)
26. Tien-Ho Chen and Wei-Kuan, Shih , "A Robust Mutual Authentication Protocol for Wireless Sensor Networks" *ETRI Journal*, Volume 32, Number 5, October 2010
27. Vinit Garg, Manoj Kr.Shukla, Tanupriya Choudhury, Charu Gupta, "Advance Survey of Mobile Ad-Hoc Network," *IJCST Vol. 2, Iss ue 4, Oct . - Dec. 2011*