MANET Its Vulnerability Challenges and Security Attacks and Routing Protocols

Sashi Bhusan Maharana¹, Latha Padhy², B. Pramila Rani³, N. Saranaya Devi⁴
¹,²,³,⁴Centurion University of Technology and Management, Paralakhemundi, INDIA

ABSTRACT
In Mobile ad hoc network (MANET) all nodes are battery-operated; as battery power or batter energy is incomplete resource therefore it needs special attention to minimize energy consumption in MANET. For MANETs, optimization of energy ingesting has greater impact as it straightly corresponds to lifetime of networks. In WSN, sensor nodes have a partial storage capacity and limited transmission range. Maintenance of routes in wireless sensor network is the accountability of the routing protocols. In this paper we discuss about the various routing protocols, benefits, and challenges behavior in MANET.

Keywords--- Adhoc Network, Sensors, WSN

I. INTRODUCTION
Wireless sensor network (WSN) is generally considered as one of the most significant Technologies for the twenty-first century. In the past years, it has established tremendous attention from both academia and industry all over the world. A WSN naturally consists of a large number of low cost, low-power, and multifunctional wireless sensor nodes, with sensing, wireless communications and addition capabilities. These sensor nodes interconnect over short distance via a Wireless medium and collaborate to complete a common task, ex: environment monitoring, military surveillance and industrial process control. The basic thinking is to behind WSNs is that, while the capability of each sensor node is limited, the aggregate power of the whole network is sufficient for the required mission. In many WSN applications, the deployment of sensor nodes is performed in an ad hoc fashion without careful planning and engineering. Once deployed, the sensors receive this packet. Using gossiping, a given sensor would receive only one copy of a packet being sent while gossiping tackles the implosion problem, there is an important delay for a packet to reach all sensors in a network. Moreover, these inconveniences are highlighted when the number of nodes in the network increases.

II. BENEFITS OF MANET
A. The traditional routing protocols have some Shortcomings when applied to WSNs, which are mostly due to the energy-constrained nature of such networks. For example, flooding is a method in which a given node broadcasts data and control the packets that it has established to the rest of the nodes in the network. This process replications until the
1. Sensor nodes are typically randomly deployed and unconventionally configure themselves into a communication network Wireless sensor
networks have the following unique characteristics and constraints.

2. Sensor nodes are typically deployed and it can be numerous orders of magnitude higher than that in a MANET.

3. Sensor nodes are usually powered by battery and are positioned in a harsh environment where it is very hard to change or recharge the batteries.

4. Sensors nodes are having highly imperfect energy, computation, and storage capabilities. The sensors and recharge their batteries. Additionally, when the energy of a sensor reaches a certain threshold, the sensor will become faulty and will not be able to meaning properly, which will have a main impact on the network performance. Thus, routing protocols designed for sensors should be as energy efficient as possible to extend their lifetime and hence prolong the network lifetime while ensuring good performance overall.

5. Since sensor nodes are prone to physical damages or failures due to its deployment in harsh or hostile environment. Multiple source sensor nodes to a particular sink, exhibiting a many-to-one traffic sink, exhibiting a many-to-one traffic pattern.

6. Network topology changes repeatedly due to the node failures, damage, addition, energy depletion, or channel fading.

B. Additional challenge that faces the design of routing protocols is to accomplish the locations of the sensors. Most of the proposed protocols assume that the sensors either are prepared with global positioning system (GPS) receivers or use some localization performance to learn about their locations.

C. In addition to partial energy capacity, sensor nodes have also partial processing and storage capacities, and thus can only achieve limited computational functionalities. These hardware constraints current many challenges in software development and various security schemes network protocol design for sensor networks, which must consider not only the energy constraint in sensor nodes, but also the dispensation and storage capacities of sensor nodes.

D. Sensor node placement in WSNs is application dependent and can be moreover manual or random which finally affects the performance of the routing protocol. In maximum applications, sensor nodes can be scattered randomly in an intended area or dropped immensely over an inaccessible or hostile region. If the resultant distribution of nodes is not uniform, optimal clustering becomes essential to allow connectivity and enable energy efficient network operation. Network. To reduce the conceivable overhead in the network protocol uses Multipoint Relays (MPR). The idea of MPR is to reduce flooding of broadcasts by dropping the same broadcast in some regions in the network, more details about MPR can be found later in this chapter. Additional reduce is to provide the shortest path. The reducing the time interval for the control messages transmission can bring more reactivity to the topological changes.

III. MANET VULNERABILITIES

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user’s identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

Lack of centralized management: MANET doesn’t have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not easy to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.

Resource availability: - Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to attacks, leads to development of various attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

Scalability: - Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

Cooperativeness: - Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

Dynamic topology: - Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes.

The trust may also be disturbed if some nodes are detected as compromised. This dynamic behaviour could be better protected with distributed and adaptive security mechanisms.

Limited power supply: - The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

Bandwidth constraint: - Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

Adversary inside the Network: - The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously.
This is hard to detect that the behaviour of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.

**No predefined Boundary:** In mobile ad-hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless.

**IV. BROADCASTING APPROACHES IN MANET**

In MANET a number of broadcasting approaches on the basis of cardinality of destination set:

- **Unicasting:** Sending a message from a source to a single destination.
- **Multicasting:** Sending a message from a source to a set of destinations.
- **Broadcasting:** Flooding of messages from a source to all other nodes in the specified network.
- **Geocasting:** Sending a message from a source to all nodes inside a geographical region.

**V. ATTACKS IN MANET**

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information.[4] Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber-attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

1. **External Attack:** External attacks are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services.
2. **Internal Attack:** Internal attacks are from compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyse traffic between other nodes and may participate in other network activities.

**Denial of Service attack:** This attack aims to attack the availability of a node generally uses radio signal jamming and the battery exhaustion method.

**Impersonation:** If the authentication mechanism is not properly implemented a malicious node can act as a genuine node and monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.

**Eavesdropping:** This is a passive attack. The node simply observes the confidential information. This information can be later used by the malicious node. The secret information like location, public key, private key, password etc. can be fetched by eavesdropper.

**Routing Attacks:** The malicious node make routing services a target because it’s an important service in MANETs. There are two flavours to this routing attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism. The first is aimed at blocking the propagation of routing information to a node. The latter is aimed at disturbing the packet delivery against a predefined path.

**Black hole Attack:** In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it [9]. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol.
Wormhole Attack: In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the networks from that point. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attacks is known as a wormhole.

Replay Attack: An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

Jamming: In jamming, attacker initially keep monitoring wireless medium in order to determine frequency at which destination node is receiving signal from sender. It then transmit signal on that frequency so that error free receptor is hindered.

Man-in-the-middle attack: An attacker sites between the sender and receiver and sniffs any information being sent between two nodes. In some cases, attacker may impersonate the sender to communicate with receiver or impersonate the receiver to reply to the sender.

Gray-hole attack: This attack is also known as routing misbehaviour attack which leads to dropping of messages. Gray hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability or the entire network. If the attack is successful the services will not be available.

VI. MANET APPLICATIONS

With the increase of portable devices as well as progress in wireless communication, ad-hoc networking is gaining importance with the increasing number of widespread applications. 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 the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANET is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. Typical applications include [12, 16].

1. Military Battlefield: Military equipment now routinely contains some sort of computer equipment. Ad-hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters. The basic techniques of ad hoc network came from this field.

2. Commercial Sector: 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 hand held. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

3. Local Level: Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.

4. Personal Area Network (PAN): Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS. The PAN is potentially a promising application field of MANET in the future pervasive computing context.

5. MANET-Volvo: A MANET enabled version of JXTA peer-to-peer, modular, open platform is used to support user location and audio streaming over the JXTA virtual overlay network. Using MANET-JXTA, a client can search asynchronously for a user and a call setup until a path is available to reach the user. The application uses a private signalling protocol based on the exchange of XML messages over MANET-JXTA communication channels.

VII. MANET CHALLENGES
Regardless of the attractive applications, the features of MANET introduce several challenges that must be studied carefully before a wide commercial deployment can be expected. These include [15, 16]:

1. **Routing:** Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive. Multi cast routing is another challenge because the multi cast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

2. **Security and Reliability:** In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to e.g. nasty neighbour relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics introduce also reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobility-induced packet losses, and data transmission errors.

3. **Quality of Service (QoS):** Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services.

4. **Inter-networking:** In addition to the communication within an ad hoc network, inter-networking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management.

5. **Power Consumption:** For most of the light-weight mobile terminals, the communication-related functions should be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration.

6. **Multicast:** Multicast is desirable to support multiparty wireless communications. Since the multicast tree is no longer static, the multicast routing protocol must be able to cope with mobility including multicast membership dynamics (leave and join).

7. **Location-aided Routing:** Location-aided routing uses positioning information to define associated regions so that the routing is spatially oriented and limited. This is analogous to associatively-oriented and restricted broadcast in ABR.

**VIII. ROUTING PROTOCOLS**

Routing is the most fundamental research issue in MANET and must deal with limitations such as high power consumption, low bandwidth, high error rates and unpredictable movements of nodes. Generally, current routing protocols for MANET can be categorized as:

1. **Proactive (Table-Driven):** The pro-active routing protocols [11,14] are the same as current Internet routing protocols such as the RIP (Routing Information Protocol), DVM (distance-vector), OSPF (Open Shortest Path First) and link-state. They attempt to maintain consistent, up-to-date routing information of the whole network. Each node has to maintain one or more tables to store routing information, and response to changes in network topology by broadcasting and propagating. Some of the existing proactive ad hoc routing protocols are: DSDV (Destination Sequenced Distance-Vector, 1994), WRP (Wireless Routing Protocol, 1996), CGSR (Cluster head Gateway Switch Routing, 1997), GSR (Global State Routing, 1998), FSR (FishEye State Routing, 1999), HSR (Hierarchical State Routing, 1999), ZHLS (Zone based Hierarchical Link State, 1999), STAR (Source Tree Adaptive Routing, 2000).

2. **Reactive (Source-Initiated On-Demand Driven):** These protocols try to eliminate the conventional routing tables and consequently reduce the need for updating these tables to track changes in the network topology. When a source requires to a destination, it has to establish a route by route discovery procedure, maintain it by some form of route maintenance procedure until either the route is no longer desired or it becomes inaccessible, and finally tear down it by route deletion procedure. Some of the existing re-active routing protocols are [12,14]. DSR (Dynamic Source Routing, 1996), ABR (Associatively Based Routing, 1996), TORA (Temporally-Ordered Routing Algorithm, 1997), SSR (Signal Stability Routing, 1997), PAR (Power-AwareRouting, 1998), LAR (Location Aided Routing, 1998), CBR (Cluster Based Routing, 1999), AODV (ad hoc On-Demand Distance Vector Routing, 1999). In pro-active routing protocols, routes are always available (regardless of need), with the consumption of signalling traffic and power. On the other hand, being more efficient at signalling and power consumption, re-active protocols suffer longer delay while route discovery. Both categories of routing protocols have been improving to be more scalable, secure, and to support higher quality of service.

3. **Hybrid Protocols:** Hybrid routing protocols [11, 12] aggregates a set of nodes into zones in the network topology. Then, the network is partitioned into zones and proactive approach is used within each zone to maintain routing information. To route packets between different zones, the reactive approach is used. Consequently, in hybrid schemes, a route to a destination that is in the same zone is established without delay, while a route discovery and a route maintenance procedure is required for destinations that are in other zones. The zone routing
protocol (ZRP) and zone-based hierarchical link state (ZHLS) routing protocol provide a compromise on scalability issue in relation to the frequency of end-to-end connection, the total number of nodes, and the frequency of topology change. Furthermore, these protocols can provide a better trade-off between communication overhead and delay, but this trade-off is subjected to the size of a zone and the dynamics of a zone. Thus, the hybrid approach is an appropriate candidate for routing in a large network. At network layer, routing protocols are used to find route for transmission of packets. The merit of a routing protocol can be analysed through metrics—both qualitative and quantitative with which to measure its suitability and performance. These metrics should be independent of any given routing protocol. Desirable qualitative properties of MANET are Distributed operation, Loop-freedom, Demand-based operation, Proactive operation, Security, Sleep period operation and unidirectional link support. Some quantitative metrics that can be used to assess the performance of any routing protocol are End-to-end delay, throughput, Route Acquisition Time, Percentage Out-of-Order Delivery and Efficiency. Essential parameters that should be varied include: Network size, Network connectivity, Topological rate of change, Link capacity, Fraction of unidirectional links, Traffic patterns, Mobility, Fraction and frequency of sleeping nodes [1,9,10].

IX. SECURITY OF MANET

The goal of system security is to have controlled access to resources. The key requirements for networks are confidentiality, authentication, integrity, non-repudiation, and availability [13, 14].

- **Confidentiality**: It protects data or a field in message. It is also required to prevent an adversary from traffic analysis.
- **Integrity**: It ensures that during transmission the packets are not altered.
- **Authorization**: It authorizes another node to update information or to receive information.
- **Availability**: It ensures that services are available whenever required.
- **Resilience to attacks**: It is required to sustain the network functionalities when a portion of nodes is compromised or destroyed.
- **Freshness**: It ensures that malicious node does not resend previously captured packets.
- **Anonymity**: This service helps for data confidentiality and privacy.
- **Access control**: It prevents unauthorised access to a resource.
- **No repudiation**: No repudiation prevents the source from denying that it sends the packet.

X. CONCLUSION AND FUTURE SCOPE

The future of ad-hoc networks is really appealing, giving the vision of—anytime, anywhere—and cheap communications. Before those imagined scenarios come true, huge amount of work is to be done in both research and implementation. At present, the general trend in MANET is toward mesh architecture and large scale. Improvement in bandwidth and capacity is required, which implies the need for a higher frequency and better spatial spectral reuse. Propagation, spectral reuse, and energy issues support a shift away from a single long wireless link (as in cellular) to a mesh of short links (as in ad-hoc networks). Large scale ad hoc networks are another challenging issue in the near future which can be already foreseen. As the involvement goes on, especially the need of dense deployment such as battlefield and sensor networks, the nodes in ad-hoc networks will be smaller, cheaper, more capable, and come in all forms. In all, although the widespread deployment of ad-hoc networks is still year away, the research in this field will continue being very active and imaginative.

REFERENCES

[5] Guoyou He, —Destination – Sequenced DistanceVector (DSDV) Protocoll‖, Networking Laboratory, Helsinki University of Technology, ghe@cc.hut.fi.