MOBILE AD – HOC NETWORK (MANET): VULNERABILITIES, APPLICATIONS & SECURITY ISSUES

M.A Siddique[1], Sarah Khan[2]

Abstract: Mobile ad-hoc network (MANET) is one of the most promising fields for research and development of wireless network. 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 severe challenges, the special features of MANET bring this technology great opportunistic together. This paper describes the fundamental problems of ad hoc network by giving its related research background including the concept, features, status, 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.

Keywords: MANET, Wireless Networks, Ad hoc Networking, Routing Protocol.

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an ―infrastructure less network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad-hoc network is self-organizing and adaptive. The set of applications for MANETs 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. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET is more prone to malicious attacks.

2. RELATED WORK

A MANET is a most promising and rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its great features, MANET attracts different real world application areas where the networks topology changes very quickly. However, in many researchers are trying to remove main weaknesses of MANET such as limited bandwidth, battery power, computational power, and security. The existing security solutions of wired networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security

attacks. In this paper, we have discussed vulnerabilities, application, and security aspects in MANET. In this paper we also discuss challenging issue and future of MANET.

3. 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: (a) Lack of centralized management, (b) Resource availability, (c). Scalability, (d). Dynamic topology, (e). Limited power supply, (f). Bandwidth constraint, (g). Adversary inside the Network, (h). No predefined Boundary, (I). Security Goals.

4. BROADCASTING APPROACHES IN MANET:

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

(i) **Unicasting:** Sending a message from a source to a single destination.

(ii) **Multicasting:** Sending a message from a source to a set of destinations.

(iii) **Broadcasting:** Flooding of messages from a source to all other nodes in the specified network.

(iv) **Geocasting**: Sending a message from a source to all nodes inside a geographical region.

5. 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. 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:

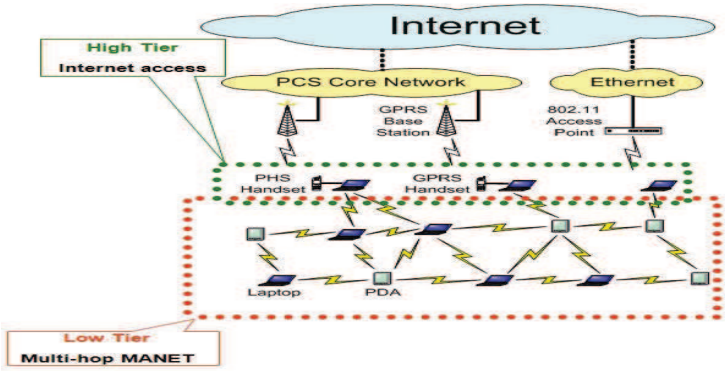
(a) External Attack:

(b) 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 analyze traffic between other nodes and may participate in other network activities.

Denial of Service attack, Impersonation, Eavesdropping, Routing Attacks, Black hole Attack, Worm hole Attacks, Replay Attack, Jamming, Man- in- the- middle attack, Gray-hole attacks.

6. MANET APPLICATIONS

a. Military Battlefield
b. Commercial Sector
c. Local Level
d. Personal Area Network (PAN)
e. MANET-VoVoN



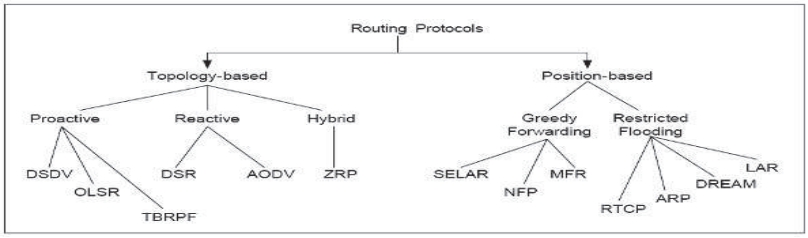
7. MANET CHALLENGES

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 :

1: Routing
2: Securities and Reliability
3: Quality of Service (QoS)
4: Inter-networking
5: Power Consumption
6: Location-aided Routing

8. 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:



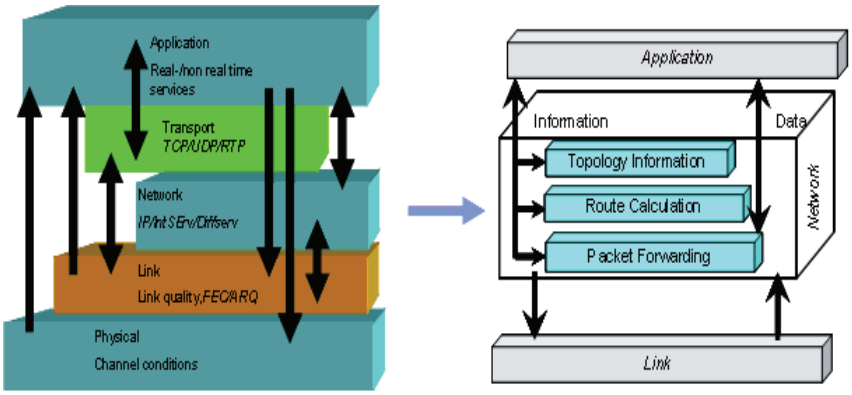
8.1 Proactive (Table-Driven): The pro-active routing protocols [11,14] are the same as current Internet routing protocols such as the RIP(Routing Information Protocol), DV(distance-vector), OSPF (Open Shortest Path First) and link-state . They attempt to maintain consistent, up-to-date routing information 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 pro-active 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).

8.2 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 (Associativity Based Routing, 1996), TORA (Temporally-Ordered Routing Algorithm, 1997), SSR (Signal Stability Routing, 1997), PAR (Power-Aware Routing,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 signaling traffic and power. On the other hand, being more efficient at signaling and power consumption, re-active protocols suffer longer delay while route discovery. Both categories of routing protocols have been improving g to be more scalable, secure, and to support higher quality of service.

8.3 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 analyzed 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.

9.. CRYPTOGRAPHY BASED SECURE ROUTING STRATEGIES IN MANET:



(i) Ariadne: It is a secure reactive (on-demand) routing protocol based on DSR that provides authentication of routing messages. Authentication can be performed by using shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signatures. Ariadne is based on the *Timed Efficient Stream Loss-tolerant Authentication* (TESLA) protocol

(ii) SAODV: It was introduced to protect the routing messages of the original AODV protocol. In SAODV, digital signatures are used to authenticate RREQ and RREP messages and hash chains are used to authenticate the hop-count fields within the RREQ and RREP messages.

(iii) The SAR protocol: It incorporates security attributes as parameters into ad hoc route discovery. It enables the use of security as a negotiable metric with the intention to improve the relevance of the discovered routes. While AODV discovers the shortest path between two nodes, SAR can discover a path with desired security attributes. For instance, the criteria for a valid route can be that every node in the route must own a particular shared key. In such a case, routing messages would be encrypted with the source node's shared key and only the nodes with the correct key

can read the header and forward that routing message. As a result, if a routing message reaches the destination, it must have been traveled through nodes having the same trust level as the source node. It is then for the node initiating the route discovery to decide upon the desired security level for that route.

(iv) The purpose of the ARAN protocol: It is to detect and protect against malicious actions by third parties and peers. It provides authentication, message integrity, and non-repudiation. ARAN can be used in two different security stages: a simple mode which is mandatory and an optional stage which provides stronger security but also more overhead and is not suitable on mobile devices with very low processing or battery capacity. ARAN uses crypto-graphic certificates for authentication and non-repudiation. Each routing message is signed by the source node and broadcasted to all neighbors. An intermediate node removes the certificate and signature of the previous hop and replaces them with its own.

(v) SEAD: It is a proactive routing protocol based on DSDV. SEAD uses a hash chain method for checking the authenticity of data packets and the hash chain value is used for transmitting routing updates. The authentication of each entry of a routing update message is verified by a receiving node.

(vi) The main functionality of SLSP: It is to secure the discovery and the distribution of link state information by using asymmetric keys. SLSP consists of three major steps: public key distribution, neighbor discovery, and link state updates. Public keys are distributed between a node and all its neighbors. A central server for key distribution is thus not needed. Periodic hello messages, used in neighbor discovery, are signed using the private key of the sender. Signed link state update messages are identified by the IP address of the initiating node and include a sequence number.

(vii) SRP: It is a protocol designed to secure ZRP but can also be used with pure reactive routing protocols. A *security association* (SA) is required between a source node and a destination node. It is assumed that the SA can be established by using a shared key between the two communicating nodes. SRP uses an additional header to the underlying on-demand routing protocol packet. The header contains a sequence number QSEC, an ID number QID, and a MAC field where the output of a key hashed functions is inserted. A route request messages is discarded by intermediate nodes if the SRP header is missing.

10. CONCLUSION AND FUTURE SCOPE

The future of ad- hoc networks is really appealing, giving the vision of anytime, anywhere 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 towards 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.

11. ACKNOWLEDGMENT

The authors gratefully acknowledge the work and assistance of our colleagues and students: TVS Prasad Gupta sir, Aishwarya vayu, Priya Raja, Divya Raja, Nandini. "Authors are thankful to there parents for there love and affection".

12. REFERENCES

1. IIyas, M., 2003. The hand book of ad -hoc wireless networks. CRC press LLC.
2. B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto, and N. Kato,"A survey of routing attacks in manet," *IEEE Wireless CommunicationsMagazine*, vol. 14, no. 5, pp. 85–91, October 2007.
3. L. X. Cai, L. Cai, X. Shen, J. W. Mark, and Q. Zhang, "Mac protocol design and optimization for multi-hop ultra-wideband networks," *IEEE on Wireless Communications*, vol. 8, no. 8, pp. 4056-4065, August 2009.
4. A. Goldsmith, M. Effros, R. Koetter, M. Medard, A. Ozdaglar, and L. Zheng, "Beyond shannon: The quest for fundamental performance limits of wireless ad hoc networks," *IEEE Communications Magazine*, vol. 49, no. 5, pp. 195–205, May 2011.
5. Y.Hu, A Perrig and D. Johnson, Ariadne: A secure On-demand Routing Protocol for Ad Hoc Networks, in Proceeding of ACM MOBICOM'02, 2002.
6. K. Sanzgiri, B. Dahill, B.N. Levine, C. shield and E.M Belding- Royar, A secure routing protocol for Ad Hoc Networks, in Proceedings of ICNP'02, 2002.
7. Y. Hu, D. Johnson and A Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wire
8. D.Johnson and D. Maltz, .Dynamic Source Routing in Ad Hoc Wireless Networks,. Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

****

---

[1]Author 1:
Mohammed Ahtesham Siddique, Associate Professor, Dept of CSE,
Vijay Rural Engineering College, Nizambad (Dist), A.P, India.
Ahtesham.siddique@gmail.com

[2]Author 2:
Sarah Khan, Associate Professor, Dept of CSE,
Vijay College of Engineering for women, Nizamabad (Dist), A.P, India.
Siddiqui.sarah04@gmail.com