ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 7, July 2014

A Review on Various Protocols and Security Issues in MANET

Er.Sunaina Bagga[1], Er.Kaushik Adhikary[2]

Assistant Professor, IT, RIMT-MAEC, Mandigobingarh, India[1]

Assistant Professor, CSE, RIMT-MAEC, Mandigobingarh, India[2]

Abstract: Wireless Sensor Network (WSN) is a collection of large number of miniature devices called sensors nodes. These sensor nodes perform as router in order to communicate with each other. A Mobile Ad Hoc Network (MANET) is collection of autonomously self-organized mobile nodes. In a mobile ad hoc network, nodes communicate with each other using wireless links without pre-existing infrastructure support. Since these nodes move arbitrarily, thus they may experience rapid and unpredictable topology changes. It is quite difficult to find out which protocols may perform best under a number of different network scenarios such as network size and topology etc. The goal of my paper is to present a compressive review of the on various aspects of MANET.

Keywords: Sensor Network, MANET (Mobile Ad hoc Network), Routing Protocol, Security

I. INTRODUCTION

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless data transmission is ubiquitous. The wireless network can be classified into two types:

A. Infrastructured wireless network

In Infrastructured wireless networks the mobile node can move while communicating, the base stations are fixed and as the node goes out of the range of a base station, it gets into the range of another base station.

B. Infrastructureless or Ad Hoc wireless network

The mobile node can move while communicating, there are no fixed base stations and all the nodes in the network act as routers. The mobile nodes in the Ad Hoc network dynamically establish routing among themselves to form their own network 'on the fly'. A sensor network is defined as a composition of a large number of low cost, low power multifunctional sensor nodes which are highly distributed either inside the system or very close to it. Nodes which are very small in size consist of sensing, data processing and communicating components. The position of these tiny nodes need not be absolute; this not only gives random placement but also means that protocols of sensor networks and its algorithms must possess self organizing abilities in inaccessible areas.

A wireless sensor network is made up of three components: Sensors Nodes, Task Manager Node (User) and Interconnect Backbone. The wireless sensor networks will have wide range of application areas to make sensor networks an integral part of our lives. The big challenges for different flavors of ad-hoc networks are the need to tailor in-network data processing and communication to the varying requirements of specific applications.

Wireless Sensor Network (WSN) is type of network which consists of collection of tiny device called sensors nodes. The nodes acts as router and communicate to each other. The term 'node' or 'sensor node' will be used here to refer to a single physical device consisting of sensors, a transceiver, and supporting electronics, which is connected to a larger wireless network. Sensor node has a resource constraint (i.e. battery power, storage and communication capability). To form network, these sensor nodes are set with radio interface by which they are communicated with one to another. Sensor technology has made WSN possible that have wide and varied application. While choosing the right sensor for an application a number of characteristics are important. The important characteristics of WSNs are:

1. Less power consumption
2. Ability to cope with node
3. Failures Mobility of nodes
4. Communication failures
5. Heterogeneity of nodes
6. Usability in large scale
7. Withstand in unfavorable environmental conditions Ease of use

The WSN is built of few to several hundreds or even thousands of sensors of nodes, where each node is connected to one (or sometimes several) sensors.

1. Sensor nodes mainly use broadcast communication whereas ad hoc network uses point to point communication.
2. The topology of a sensor network changes very frequently.
3. Sensor nodes may not have global identification because of the large amount of overhead and large number of sensors.
4. The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in adhoc network.

II. FACTORS THAT AFFECT SENSOR NODES

Efforts have been made on cryptography, key management, secure routing, secure data aggregation, and intrusion detection in WSNs; there are still some challenges to be addressed.

First, the selection of the appropriate cryptographic methods depends on the processing capability of sensor nodes, indicating that there is no unified solution for all sensor networks. Instead, the security mechanisms are highly application-specific.

Second sensors are characterized by the constraints on computation capability, memory and communication bandwidth. The design of security services in WSNs must satisfy these constraints. Third, most of the current protocols assume that the sensor nodes and the base station are stationary. However, there may be situations, such as battlefield environments, where the base station and possibly the sensors need to be mobile. The mobility of sensor nodes has a great influence on sensor network topology and thus raises many issues in secure routing protocols. Some future sensor network topology and thus raises many issues in secure routing protocols

III. MANET

Ad hoc Networks (MANETs) use portable devices such as mobile phones, laptops or personal digital assistants MANETs can be exploited in a wide area of applications like military, battlefields, emergency search and rescue, law enforcement, commercial, local and personal contexts. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently.

A wireless ad hoc network is a decentralized type of wireless network.,[1] The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data.

A mobile ad hoc network is a self-configuring infrastructure less network of mobile devices connected by wireless. The dynamic nature of these networks demands new set of networking strategies to be implemented in order to provide efficient end-to-end communication. Mobile Ad Hoc Network (MANET) is collection of multi-hop wireless mobile nodes that communicate with each other without centralized control or established infrastructure. The wireless links in this network are highly error prone and can go down frequently due to mobility of nodes, interference and less infrastructure. Therefore, routing in MANET is a critical task due to highly dynamic environment.

An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks. Wireless and Mobile ad-hoc Networking covers a broad variety of applications, including areas like mesh net-working, wireless sensor networks, vehicular networks, personal area networks, some forms of body area networks and many more. A Mobile Ad hoc Network is an autonomous network that can be formed without the need of any established infrastructure or centralized administration. Ad hoc Networks is limited to stand-alone isolated networks. Various routing protocols have been proposed for MANETs [2]. But one drawback of MANETs is that communication is limited to the Ad Hoc domain only. Many applications however need a connection to an external network, like the internet.

But connectivity of a mobile Ad hoc network to the Internet is also desirable as more and more applications and services in our society now depend on fixed infrastructure networks. It is therefore important that dynamically deployed wireless Ad hoc networks should also gain access to these fixed networks and their services. The integration of MANETs into Internet increases the networking flexibility and coverage of existing infrastructure networks. When an Ad hoc network is connected to Internet, it is important for the mobile nodes to detect efficiently available Internet gateways providing access to the internet. Internet gateway discovery time and handover delay have strong influence on packet delay and throughput. The key challenge in providing connectivity is to minimize the overhead of mobile IP and Ad hoc routing protocol between Internet and Ad hoc networks [3].

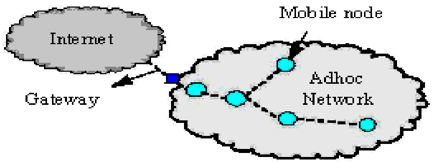

Fig. 1 Mobile Ad Hoc network connected with Internet

As illustrated in Fig. 1, in order to provide internet connectivity to the nodes in an Ad hoc network, routers or one or more nodes in the Ad hoc network can serve as Internet gateways to an external network, where the external network can be an infrastructured network such as LAN, Internet or a cellular network [6], or even an infrastructure-less network such as another Ad Hoc network. When connecting MANETs with the Internet, the routing interoperability becomes a crucial challenge. Ad Hoc nodes can not obtain routing information beyond the scope of the MANET. Therefore, the interoperability between IP routes and Ad Hoc routing needs to be given attention. When an Ad Hoc network is connected to the internet, it is important for the mobile nodes to detect efficiently available Internet Gateways providing access to the Internet. Internet gateway discovery time and handover delay have strong influence on packet delay and influence on packet delay and throughput. The key challenge in providing connectivity is to minimize the overhead of mobile IP and Ad hoc routing protocol between internet and Ad hoc networks.

Ad-hoc networks meet the requirements of spontaneous deployment, independence from any kind of existing infrastructure, and robustness in the sense of selforganization and self-healing. However, in larger deployments, quality of service for different applications and priorities of single users are additional requirements. Furthermore, the public safety domain must always be prepared for sudden changes and spontaneous events. Therefore, requirements and priorities may change over the time. Thus, the applications as well as the network have to be able to adapt to the new situation—which, in turn, requires the protocol stack in all nodes to react in highly application-specific ways. This is very hard to implement in a protocol stack where forwarding nodes are application-agnostic. Context-adaptive networking allows to take these application requirements into account in all nodes, without sacrificing a clean system architecture.

IV. ROUTING PROTOCOL IN MANET

MANETs have several routing protocols and for nearly every protocol further extensions and improvements exist, which often require particular configurations for optimal operation. The problem of finding an ideal parameter set for a given network scenario is often solved with time-consuming network simulations. However, real world deployments of Mobile Ad-hoc Networks (MANETs) require a timely determination of suitable parameters. Therefore, we propose an analytical approach to help finding appropriate parameters for a given scenario and to reduce the complexity of simulations. Most of the routing protocols require location information for sensor nodes[4] in wireless sensor networks to calculate the distance between two particular nodes on the basis of signal strength so that energy consumption can be estimated[7]. Because nodes in a MANET normally have limited transmission ranges, some nodes cannot communicate directly with each other. Hence, routing paths in mobile ad hoc networks potentially contain multiple hops, and every node in mobile ad hoc networks has the responsibility to act as a router.

Single-path routing approach is unable to provide efficient high data rate transmission in wireless sensor networks due to the limited capacity of a multi-hop path and the high dynamics of wireless links. This problem can be overcome by using multipath routing. Routing protocols define a set of rules which governs the journey of message packets from source to destination in a network. In MANET, there are different types of routing protocols each of them is applied according to the network circumstances. A routing protocol is needed whenever a packet needs to be transmitted to a destination via number of nodes and numerous routing protocols have been proposed for such kind of ad hoc networks. These protocols find a route for packet delivery and deliver the packet to the correct destination[8]. The studies on various aspects of routing protocols have been an active area of research for many years. Many protocols have been suggested keeping application and type of network in view.

V. CLASSIFICATION OF PROTOCOLS

MANET or routing protocols can be broadly classified into three categories such as Table Driven Protocols or Proactive Protocols, On-Demand Protocols or Reactive Protocols, Hybrid Protocol.

A. .Table Driven or Proactive Routing Protocols

Proactive routing protocols are also called as table driven routing protocols. In this each node maintain routing table which contains information about the network topology even without requiring it. The routing tables are updated periodically whenever the network topology changes. In the proactive protocol all the nodes maintains the information about the next node. All the nodes of any protocol have to relay it's entire to its adjacent nodes. The nodes send the packet data from one node to the other node after mutual agreement therefore the entire node constantly update their position. Proactive protocols are not appropriate for large networks as they need to maintain node entries for each and every node in the routing table of every node. Network mobility is another factor that can degrade the performance of certain protocols. When the network is relatively static, proactive routing protocols can be used, as storing the topology information is more efficient. There are various proactive routing protocols. Example: DSDV (Dynamic Destination- Sequence Distance-Vector Routing Protocol), OLSR (Optimized Link State Routing), WRP (Wireless Routing Protocol) etc.

B. On Demand Protocol or Reactive Routing Protocols

Reactive protocol also called as on demand routing protocol. Reactive protocol is based upon some sort of query reply dialog. Reactive protocol is better than the proactive protocol .Reactive routing is best adapted to the most challenging incarnations of the adhoc networks[15]. Their major goal is to minimize the network traffic overhead. Most of time everyone can use the reactive protocol because it is an on demand routing protocol. .As the mobility of nodes in the network increases, reactive protocols perform better. The mobility and traffic pattern of the network must play the key role for choosing an appropriate routing strategy for a particular network. In this type of protocol, route is discovered whenever it is needed. Nodes initiate route discovery when demanded. A route is acquired by the initiation of a route discovery process by the source node. Examples: DSR (Dynamic Source Routing), AODV (Adhoc on Demand Distance Vector), TORA (Temporary Ordered Routing Protocol).

C. Hybrid Routing Protocols

This type of protocol is a trade-off between proactive and reactive protocols. Proactive protocols have more overhead and less latency while reactive protocols have less overhead and more latency. Thus a Hybrid protocol is needed to overcome the shortcomings of both proactive and reactive routing protocols. This protocol is a combination of both proactive and reactive routing protocol. It uses the on demand mechanism of reactive protocol and the table maintenance mechanism of proactive protocol so as to avoid latency and overhead problems in the network.

Hybrid protocol is based upon distance vector protocol but contain many features and advantage of link state protocol. Hybrid protocol enhances interior gateway routing protocol. Hybrid protocol is appropriate for large networks where large numbers of nodes are present. In this, large network is divided into a set of zones where routing inside the zone is done by using proactive approach and outside the zone routing is done using reactive approach. It is more appropriate to apply a hybrid protocol rather than a strictly proactive or reactive protocol as hybrid protocols often possess the advantages of both types of protocols. There are various hybrid routing protocols for MANET like ZRP (Zone Routing Protocol), SHARP (Sharp Hybrid Adaptive Routing Protocol, DHAR (Dual-Hybrid Adaptive Routing), ADV (Adaptive Distance Vector Routing) etc.

VI. OTHER ROUTING PROTOCOL

A.Multipath Routing Protocol

Due to the limited capacity of a multi-hop path and the high dynamics of wireless links, single-path routing approach is unable to provide efficient high data rate transmission in wireless sensor networks [9]. Nowadays, the multipath routing approach is broadly utilized as one of the possible solutions to cope with this limitation. This section discusses some of the multipath routing protocols.

B. Optimized Link State Routing Protocol (OLSR)

OLSR is a popular routing protocol for MANETs. As a proactive routing protocol it maintains routes to all possible destinations all the time. The overall performance of an OLSR network is highly influenced by the transmission interval of topology control messages. Depending on the mobility of the nodes and the available bandwidth, shorter or longer intervals are more appropriate. The results allow for a precise estimation of the load imposed by OLSR control messages for each node. This eliminates the need of time-consuming simulations to choose appropriate intervals for control messages. Furthermore, these predictions could be a basis for automatic protocol configuration during runtime.

C. Link State Routing Protocols (LSRs) - LSR, OLSR performs neighbor detection and advertises links in the network with two different message types. HELLO messages are used to discover links to neighboring nodes, while Topology Control (TC) messages are used to disseminate this topology information throughout the network

D. Routing Internet Protocols

Routing in Internet is IP address based. Each IP address consists of network id and host id portion. Routing decisions are taken by routers for packets based on the network id portions of the destination IP addresses. The IP addresses of nodes within the same network thus share the common network id whereas the node address portion of the IP address identifies a specific node in the network. The highest level of the Internet hierarchy consists of a number of Autonomous Systems. Each Autonomous System is a distinct routing domain. Routers communicate with each other within an Autonomous System using intra-domain routing protocols, which are also known as Interior Gateway Protocols. Gateway routers are used to interconnect different Autonomous Systems. Exterior Gateway Protocols are used to exchange routing information between Autonomous Systems. Routing information Protocol (RIP) and Open Shortest Path First (OSPF) may be used as Interior gateway protocols. OSPF is a member of the “link state” family and commonly used nowadays. It uses multi-metrics of a link that may consider bandwidth, hop count, and reliability. A router in OSPF is aware of all links between all routers of an Autonomous System. In this, routers maintain a map of the whole network that is updated if a change in the network topology is detected. The routers in OSPF calculate shortest/best path from source to destination.

Border Gateway Protocol (BGP) provides connectivity between different Autonomous Systems and also provides sharing of routing information by one Autonomous System with other Autonomous System. It exchanges routing tables to other Autonomous Systems on demand.

VII. SECURITY ISSUES

The routing protocol is based on the following quality of service parameters like delay, jitter, routing overhead, route acquisition time, throughput, hop count, packet mobility delivery ratio using manhattans grid and random waypoint models. The main aim is to find out the payload a node has to pay to guarantee the good quality. Continuous stream security in WSNs: current work on security in sensor networks focuses on discrete events such as temperature and humidity.. Video and image sensors for WSNs might not be widely available now, but will be likely in the future.

QoS and security: performance [10] is generally degraded with the addition of security services in WSNs. Security in WSNs focus on individual topics such as key management, secure routing, secure data aggregation, and intrusion detection. QoS and security services need to be evaluated together in WSNs. Substantial differences in authentication and encryption exist between discrete events and continuous events, indicating that there will be distinctions between continuous stream security and the current protocols in WSNs

Some future trends in WSN security research are identified as follows: Exploit the availability of private key operations on sensor nodes: recent studies on public key cryptography [11]have shown that public key operations may be practical in sensor nodes. However, private key operations are still very expensive to realize in sensor nodes. A public key cryptography can greatly ease the design of security in WSNs, improving desirable. Secure routing protocols for mobile sensor networks has a great influence on sensor network topology and thus on the routing protocols. Mobility can be at the base station, sensor nodes, or both. Current protocols assume the sensor network is stationary. New secure routing protocols for mobile sensor networks need to be developed. The lifetime [5] of the routing security in sensor networks focuses on discrete events such as temperature and humidity

There are different ways by which we can classify the sensor networks routing protocols. According to network structure, these routing protocols can be classified as flat, hierarchical, and location-based protocols. Also, these protocols can be classified into multipath-based, query-based, negotiation-based Quality of Service (QoS)-based or coherent based depending on the protocol operation. Moreover, these protocols can be classified into three categories, namely, reactive, proactive, and hybrid protocols depending on route discovery.

Due to its unique characteristics, MANETs are suffering from a wide range of security threats and attacks ,unsecured wireless channels ,Dynamic mobility, limited resources, Routing attacks in MANET etc. Finally, some challenges are also mentioned which need in depth investigation to secure MANET. These requirements are very diverse: data-consistency, reliability, energy efficiency, privacy, and so forth. The requirements may even change over time, depending on the current situation and environment. The new concept of Context-adaptive Networking is to allow applications to adjust processing and communication at arbitrary points in the network, as required in the specific situation. It provides an abstraction, and therefore facilitates the adaptation to changing requirements, and the integration of new applications in the future.

In order to implement Context-adaptive Networks, a number of key challenges need to be tackled. Mechanisms to deploy functional components (i.e. slices) to network nodes are necessary. These mechanisms must be simple and robust, and it must be possible to employ them in settings where resources are very scarce. At the same time, isolation between slices needs to be considered for functional and security reasons. This includes the question of allocating scarce resources in case of competing slices—fairness and security aspects are immediately evident. On the other hand, it may be desirable to re-use components between slices for efficiency reasons. It also relates to the question how much control a slice needs about the device it is execute flexibility that is needed in order to implement demanding applications over resource-constrained.

It exchanges routing tables to other Autonomous Systems on key operations may be practical in sensor nodes. However, private key operations are still very expensive to realize in sensor nodes. As public key cryptography can greatly ease the design of security in WSNs, improving desirable. Secure routing protocols for mobile sensor networks: mobility of sensor nodes has a great influence on sensor network topology and thus on the routing protocols. Mobility can be at the base station, sensor nodes, or both. Current protocols assume the sensor network is stationary. New secure routing protocols for mobile sensor networks need to be developed.

VII. CONCLUSION

Many routing protocols have been proposed which are not suitable for all applications in WSNs. Many issues and challenges still exist that need to be solved in the routing protocol in sensor networks. Therefore, it is quite difficult to determine which protocols may perform best under a number of different network scenarios, such as increasing node density and traffic. The routing protocol with a limited but rapidly growing set of results. This paper discusses various categories on routing protocols for MANET. We provide an overview of a wide range of routing protocols and also a performance comparison of all routing protocols.

REFERENCES

[1] Anu Kumari, Arvind Kumar, Akhil Kumar,“Survey Paper On Energy Efficient Routing Protocol in MANET, IJARCSSE, March2013.

[2] Routing Protocols in Wireless Adhoc Networks: A Comparative Study R. Anderson and M. Kuhn, “Low cost attacks on tamper resistant better network resource utilization.

[3] Val Orozco, “Routing Protocols in Wireless Sensor Networks”, October 2009.

[4] Man Wah Chiang, Zeljko Zilic, Katarzyna Radecka, Jean-Samuel Chenard, “Architectures of Increased Availability Wireless Sensor Network Nodes” IEEE, Vol.2, pp 1232-1240, Feb 2004.

[5] Baranidharan and B. Santhi, “An Evolutionary Approach to improve the life time of the “Wireless sensor network”

[6] V.M.Priyadharshini, N.Muthukumar, M.Natarajan, “Cellular Architecture Sensors for Wireless Sensor Networks” IJRRSE, Vol.01 No.02, pp 47-51 June 2012

[7] Electronics and Engineering, Lovely Professional University, Phagwara, Punjab, India “A Novel Review on Routing Protocols in MANETs” under Undergraduate Academic Research Journal (UARJ), ISSN: 2278 –1129, Volume-1, Issue-1, 2012Lu Han, October 8, 2004 “Wireless Ad-hoc Networks”

[8] Ipsita Panda. “A Survey On Routing Protocols of Manets by Using QOS Metrics” IJARCSSE, Volume2, Issue 10, October 2012, pp. 120-129.

[9] “THE HANDBOOK OF AD HOC WIRELESS NETWORKS” Edited by Mohammad Ilyas Florida Atlantic University Boca Raton, Florida Signal Processing, Communication and Networking, pp. 545-550, Feb. 2007.

[10] J. Macker, “Mobile ad hoc networking (MANET):Routing protocol performance issues and evaluation considerations,” RFC 2501, IETF Network WG, 1999.[5] E. Geisberger and M. Broy, Eds.agenda Ct works. Atvol. 38, pp. 393–422, 2002.

[11] R.C. Merkle, “Protocols for public key crypto systems”, In Proceedings of the IEEE Symposium on Research in Security and Privacy, April 1980; e-mail: akush20@gmail.com

[12] “A Survey on Security Issues in Ad Hoc Routing Protocols and their Mitigation Techniques” Harshavardhan Kayarkar M.G.M’s College of Engineering and Technology, Navi Mumbai, India Email: hjkayarkar@gmail.com

BIOGRAPHIES

Er.Sunaina Bagga has done her M.Tech in IT and B.E in CSE. She is working as HOD cum Assistant Professor in RIMT-MAEC, Mandi Gobindgarh. She has 15 years of teaching experience. Her areas of interest are Wireless Network and Security.

Er.Kaushik Adhikary has done his M.Tech in CSE from MMU Mullana and B.Tech in CSE from NIT Hamirpur. He is working as Assistant Professor in RIMT-MAEC, Mandi Gobindgarh. He has 9 years of teaching experience. His area of interest is Wireless Network and Security.