Scientific Research Publishing

Communications and Network, 2016, 8, 205-218
http://www.scirp.org/journal/cn
ISSN Online: 1947-3826
ISSN Print: 1949-2421

A Novel Review on Security and Routing Protocols in MANET

Muhammad Kashif Nazir, Rameez U. Rehman, Atif Nazir

Department of Computer Science, National Textile University, Faisalabad, Pakistan
Email: kashifgcu@live.com, ramuz_malik@yahoo.com, atif.nazir1225@gmail.com

How to cite this paper: Nazir, M.K., Rehman, R.U. and Nazir, A. (2016) A Novel Review on Security and Routing Protocols in MANET. *Communications and Network*, **8**, 205-218.
http://dx.doi.org/10.4236/cn.2016.84020

Received: August 30, 2016
Accepted: September 19, 2016
Published: September 22, 2016

Abstract

The origin of Mobile ad hoc network (MANET) was started in 1970 as packet radio network (PRNET), later on different researches were made on it in different ages. MANET works under no fixed infrastructure in which every node works likes a router that stores and forwards packet to final destination. Due to its dynamic topology, MANET can be created anywhere, anytime. As there are limited resources in MANET so it faces many problems such as security, limited bandwidth, range and power constraints. Due to this, many new routing protocols are proposed. This article examines different techniques to manage congestion control, security issues, different layers attacks, routing protocols and challenges that are faced by MANET.

Keywords

Mobile Ad Hoc Networks, MANET, Security Attacks, Routing Protocols

1. Introduction

Mobile ad-hoc network is a way of communication, among different portable devices, without offering a centralized device. There is no need of any access point in mobile ad-hoc network. It is the beauty of mobile ad hoc network that mobile nodes communicate with different other node in the absence of any fixed or central infrastructure, this property of MANET makes it different and unique among all other networks.

Every node in MANET behaves as a router. They receive packets and move these packets to next hop, until all packets forwards to the final destination [1] [2].

There are two approaches regarding wireless communication, one where communication is carried out through central infrastructure. They need access points to communicate, our traditional mobile networks like WLAN, wireless local loop (WLL), universal mobile communication system (UMTS) and GSM, fit in infrastructure network.

The other approach where no central infrastructure is involved, communication is

done without any central mean. Every node itself behaves like a central device. This way of communication in which there is no infrastructure is actually mobile ad hoc network. In MANET we do not need a stable centralized structure, so they can be created anytime anywhere [1].

MANET is low in bandwidth and in dynamic shape, our popular technologies like cell phones, PDA, digital handheld devices, laptops and even an MP3 player may be the participant in MANET. We use term "mobility" for MANET, which means that one may move freely. No base station or access point participates in MANET, and it can easily be applicable that is why it is used in different military operations because MANET can be designed at run time. In case of natural disasters when all existing infrastructure is destroyed, we use MANET technologies for different rescue operations in this circumstances. Bluetooth is modern wireless technology. The goal in MANET is to design Bluetooth that may be used to connect with others [3].

MANET in future is going to introduce a revolution, because it takes us in ubiquitous age, where a user whenever and wherever may access everything he desires. A user who wishes to browse internet when he wants to share pictures, to check mail, to transfer a file may operate all operations through MANET. A traveller with portable computer can be facilitated with internet services at an airport, a public place or at station. A stranger may use GPS services and find required information about his destination. It also provides facility to researchers; they may transfer and retrieve their files anywhere and anytime. Business men can do video conferencing with one other through their cellular phone. It is observed that mobile internet users increase 20% - 50% in a year, which describes that soon the number of mobile internet users will exceeds the number of those who uses internet without portable computers.

Sensor network is one of MANET application. Sensors are positioned in a particular environment, which is to be observed, they sense this environment and send back information. Sensor network is specifically used to update about weather [4]. Data in the form of packets are transmitted in store and forwarded manner to deliver to the final destination [5].

2. Congestion Control

MANET works under limited resources in terms of bandwidth, range, and data rates. Due to these reasons a competition occurs among users of MANET which results, congestion in mobile ad hoc network. Transmission Control protocol (TCP) which is purely designed for internet while it cannot maintain the congestion control in MANET, because MANET shows some unique behavior of infrastructure less network, hence TCP cannot manage MANET congestion control as it manages in a good manner for other networks.

Generally, congestion control scheme can be classified into two types, one is single rate scheme and other is multi rate scheme, the basic difference between them is that multi rate scheme gives much more liberty to receivers to choice receiving rate as compared to single rate scheme. As links of multicast is heterogeneous, so receiver may

have more benefit in multicast session with respect to bandwidth utilization.

A new scheme for multicast congestion control is introduced here. TCP is not best suited for MANET because it is specially designed for internet. TCP is suffering from high link error rate in MANET. The other problem which is faced by this scheme is link access delay due to access competition in MANET. Another problem which is known as fairly shares bandwidth, and deals with misbehaving receivers. To address these above problems, different solutions were designed. Adjust multicast traffic concept is introduced which opposed to rely on individual receivers that they detect congestion and adjust their receiving rate as they desire. If a specific branch bottleneck then it is blocked the traffic, and if it is lightly used then free to go. At each bottleneck receivers requests will block. Limited control traffic scheme is proposed as on-the-spot information is in this scheme. For fair bandwidth utilization, this proposed strategy works better.

In this, a new and effective technique is introduced for wireless multi hop network for congestion control of traffic. This scheme follows the simple packet forwarding techniques by building a multihop back pressure. This scheme provides a solution to solve a single hop reliability and multihop backpressure congestion, this technique opposed message retransmission and unnecessary flow of messages.

MANET contain limited resources due that congestion problem occurs, another main problem is packet loss due to obstruction control, same reason, as above quoted that due to limited resources such phenomenon happened. An agent based congestion technique is introduced to address this problem. A mobile agent will move toward every node and at every time, after every visit, it will update the routing table with its own history of movement, it will also update routing table of every node. In this aspect a node is categorized into four categories from which context traffic is belonged either from background, video or voice, best effort. This strategy minimizes end-to-end delay and discovery request; also it makes balance the traffic in MANET. This strategy better works as existing scheme works, because it returns throughput with reduced delay and promise high delivery ratio.

Congestion control and jointly scheduling problem is addressed, combining the both congestion control and jointly scheduling problem, design an algorithm for them. Wireless Greedy Primal Dual (WGPD) is introduced to address the maximum utilization the bandwidth channel.

3. Security in MANET

Security of MANET is one of the major concerns with respect to support a safe and healthy communication among communicating nodes in an unfriendly environment. No infrastructure is followed by communicating nodes in ad hoc network, instead they organize themselves dynamically which results in emergence of new challenges for the basic security in applied architecture. Due to this sensitive infrastructure MANET can be directly attacked by hackers. By violating network confidentiality, eavesdroppers can approach secret information.

Furthermore, as mobile ad hoc networks are normally designed for some particular environment, security solutions designed for wired network may not be suitable for them. In contrast with traditional networks, where dedicated routers are placed to perform the basic functionality of network, MANET relies on respective nodes in order to achieve the required connection among nodes. All basic functions like routing, data forwarding and network management are performed by all alive nodes. Therefore, every node must be ready for encounters every time it desires to communicate. Encounters by compromised nodes are much more destructive because detection of compromised nodes is hard to achieve.

Providing the essential security services, for instance; confidentiality, availability, integrity, and authentication to mobile users, is the utmost aim of security solutions in MANET [6]. To accomplish these goals, secure protocols should be designed and some access control mechanism can be applied to provide a secure network for mobile device in an organization. Different researchers work on the security and access control mechanisms.

3.1. Security Issues in MANET

One major issue in MANET is the absence of centralized control. Because of this issue it is hard to define the boundary that separates the inner network from external world. This results in providing the chance to malicious attackers to interrupt network operations by ignoring the protocol specification.

Mobile nodes connectivity through multi-hop wireless channels is provided by MANET by following two steps: first, through link-layer protocol by ensuring one-hop connectivity to multiple hops; second, through protocol of network layer that expand the connectivity to various hops [6]. Data packet forwarding and ad hoc routing are two main functions of network layer. They deliver packets from source to destination by interacting with each other. Ad hoc routing protocol maintains routing states at each node by exchanging routing messages between them. However, both packet forwarding and routing operations are exposed to malicious attacks, which results in different kinds of interruptions in the network layer [6].

For certain destinations in the network the attackers can attract the traffic by attacking different routing protocols, and forward the packet on a route which may not be best or even not present in the network. The attackers can create severe network contention and network congestion by introducing routing loops in the network. Denial-of-service (DoS) is an additional form of packet forwarding attack that attacks via network layer in which garbage packets are injected into the network in large amount by attacker [6] [7]. This result in congestion in MANET as these packets wastes an important portion of the network.

3.2. Classification of Attacks

Like various networks, there are two kinds of attacks in MANET; *passive* and *active*. Passive attacks do not change the data transmitted over network, instead it attempts to

explore the sensitive information from the traffic that is routed in the network. A node that attack passively may act selfish to catch the transmitted information. Passive attackers are difficult to detect as they do not disturb the normality of network. Encryption is normally used to fight against passive attacks [8].

Active attacks create hurdles in message flow between nodes. Attackers inject the erroneous information to the network. These attacks can occur at network, transport, application or any other protocol layer [8]. Active attacks are more severe and are of two types internal and external. External attacks are executed by unauthorized source. Internal attacks are performed by selfish nodes. These attacks causes unauthorized access to network that allow the enemy to make certain alteration in network [9].

Active attacks are categorized into four groups:

Modification Attacks: These attacks disturb the overall communication among nodes by altering the data packets. Compromised nodes publicize itself in such manner that it provides shortest and smallest path to final receiver. By doing so, malicious nodes then catch routing information and use it for more attacks. Sinkhole attack is an instance of modification attack.

Dropping Attacks: In MANET, all nodes are supposed to forward packets towards the destination node. In this Attack, selfish nodes do not forward packets to any node; instead discard them to disturb the operation of network. End-to-end communication among nodes is avoided by selfish nodes, if the dropping hop is at crucial edge [10]. Several routing protocols use no such tools that detect either datagram have been sent to destination or not.

Timing Attacks: In timing attacks, attacker publicizes itself in such a way that it is closer to the final destination node, having optimal path, to attract other nodes. Hello flood and rushing attacks use this technique.

Fabrication Attacks: In this attack, without getting any analogous message the malicious user forward fake information to its neighboring nodes. In response to related legal route request message, the attackers can also send false packets.

The attributes of MANETs make them exposed to further attacks. In accordance with particular layer there are several types of attacks which differ in their nature. Attacks at different layers are defined below.

3.2.1. Attacks at Physical Layer

Eavesdropping, jamming and active Interference are the attacks that arise at physical layer. These attacks are related to hardware and they require assist from hardware resource to become affective [9].

Eavesdropping: The main target of such attacks is to access that secret data which should remain confidential all along the communication. The attackers can interrupt the communication by tuning up on the same frequency used for exchange of data between two authorized users [11].

Jamming: The aim of jamming is to create an obstruction between two interacting nodes by decreasing the radio signals to noise ratio. An attacker can win this goal by generating another stronger signal.

Active Interference: This attack blocks the wireless communication channel or crash the communication [12]. Routing protocols and duration are two key elements on which the intensity of effects of such attacks depends.

3.2.2. Attacks on Data Link Layer

Data link layer attacks can be assumed as how it will affect the status of network as a whole. These effects can be classified in terms of link breakage, path discovery failure, energy consumption and many more [9]. The improper behavior of nodes can be entirely in the attention of selfish nodes.

Traffic Analysis: Traffic monitoring and analysis is actually not an attack, instead a tool to prepare such a one. An attacker can get confidential information about the communicating nodes within the network. Such as, for how long two users are in communication with each other, as well as discover their communicating functionalities. With the help of such specific information, it is easier for a malicious node to choose how to attack a node, aiming efficiency. Against all these reasons, traffic monitoring and analysis should be considered as a sever threat to all communication security within MANET.

3.2.3. Attacks on Network Layer

The network layer in MANET use hop-by-hop strategy in order to help nodes to remain connected [9]. It is very easy for malicious attacker to attack on MANET as every single node takes routing decision to forward packet. The main idea of network layer attack is to absorb the network traffic after inserting itself in working path. The attacker can create severe congestion by introducing routing loops. Different types of attacks are categorized as follows:

Black hole Attack: In this attack, the unauthorized node tries to interrupt the communication between nodes by declaring that it has an optimal way to the target node. Once the node manages to place itself among communicating nodes, it can do anything with packets moving in the network [9].

Wormhole Attack: In this attack, malicious node gets information at one end in the network and moves it toward another attacker node. The wormhole is referred to as tunnel that exists between two malicious nodes. This is the cruelest attack. Wormholes are used by the attackers in the network to present their node as more attractive in order to route more data through them. When attacker uses wormhole attack in routing protocols like, AODV and DSR, the attack tries to avoid the detection of any way rather than through wormhole. The existing protocols are said to be unsuitable to find valid routes if protection mechanism is not applied in network routing protocols.

Sinkhole Attack: In this attack, a cooperative node gets the whole network traffic by advertising false routing information. It alters the confidential information after receiving whole network traffic e.g. modification in data packet or drop them to increase the network complexities. The performance of network is overall affected by sinkhole attacks, such as AODV by using flaws as increasing the sequence number or reducing the number of hop count. In this manner, the attacker node seems to provide optimal

path for the hops to communication [9].

3.3. Security Goals

Just like other working networks, availability, integrity, authenticity, confidentiality and non-repudiation are resilience to attacks and anonymity are also major goals of MANET.

Availability is an important attribute of network security. It ensures the availability of services, offered by the nodes, to its users, as well as make sure the survival of network devices in case of DoS attacks.

Integrity guarantees the identification of packet when it is transmitted. It ensures that packets are not modified during transmission.

Authentication guarantees that the communicating nodes and the source of information are authorized. An attacker can gain illegal access to secret information and resources and probably interfere with the operation of other parties. Authorization is normally used to allow permissions to different people.

Confidentiality means that some authentic messages are only approachable to those hops that have been allowed to access it. This makes sure the protection of secret data and information. In sensitive environments, such as military environment, the exposure of secret information can have destructive consequences.

Non-Repudiation narrates the fact that if a node in MANET sends a message then it cannot refuse to the performed activity. This activity is helpful in discovery of selfish nodes. For instance, if a node gets an erroneous message from the sender, it can use this message as a proof to notify other nodes that a certain node is compromised.

Resilience to Attacks manages to maintain the network functionality when a particular area of network is compromised to destroy.

Anonymity helps to keep data confidential and private.

3.4. Security Solutions

Proactive and reactive are two main approaches to secure a MANET. The idea of proactive strategy is to concentrate on preventing security threats mainly through different cryptographic methods. On the other hand the on demand routing strategy detects threats and takes actions accordingly.

Every strategy has its own pros and appropriate for solving various issues in the whole area. For instance, the safest routing protocol assumes the table driven approach to protect routing datagram in network whereas the on demand approach is mainly used to protect message forwarding operations.

Due to the unclear line of defense, the security solution in MANET should combine both reactive and proactive strategy and enclose detection, prevention and reaction at one place. The prevention component works by boosting the difficulty for attacker to enter into the system. However the past experience of security has straightforwardly revealed that it is quite impossible to get an entirely intrusion-free system, in spite of how correctly the mechanism of prevention is designed. This is particularly factual in

the case of ad hoc network that consist of mobile nodes that are inclined to physical capture or compromise. Thereof, the reaction and detection mechanism that invent the irregular intrusions and obtain response to prevent continuous harmful effects are crucial for the security solutions to handle in the existence of inadequate interruptions.

The prevention modules is basically carried out by secure ad hoc protocols that stop the malicious from inserting wrong situation at different hops. These routing protocols depends on DSR (Dynamic Source Routing), Destination-Sequenced Distance Vector (DSDV), AODV(Ad hoc On-demand Distance Vector)and utilize different cryptographic primitives (e.g., hash chains, digital signatures,) to validate the routing communication. The detection component finds continuing attacks by identifying the unusual behavior of malicious nodes. Such kind of misbehavior is traced either in an end-to-end manner or by neighboring hops by overhearing the medium and finally reaching mutually consensus. Once an malicious node is found, the reaction module makes arrangements in forwarding and routing process that includes prevention of node in path selection in order to exclude the hop collectively from the whole network [13].

3.5. Security Challenges

Challenges and opportunities in achieving the security goals are two main features of MANET. The security factor in adhoc networks is very essential to fulfill the basic functions like packet forwarding and routes etc.

The use of ad hoc networks is now increasing especially in sensitive areas like emergency, military etc., where security is essentially required in order to protect network from attacks by malicious nodes.

Because of dynamic nature of ad hoc network, a trusted relationship among nodes is hard to derive. As there are various types of attacks that can severely harm the MANET, so it is needed in security mechanisms to adjust and manage on-the-fly changes. Network operations can easily be affected if counter steps are not embedded into their design.

As MANET holds dynamic nature so it do not have any centralized or fixed structure, all nodes in such networks are not in direct transmission range for each other. One may not accept the present infrastructure. Setting up an infrastructure in this situation is not useful in terms of expenses and time consuming. On that account, supporting the required network services and connectivity appears a real issue.

In a MANET mobile nodes exchange variable number of datagram along different paths builds up by many routing algorithms in order to communicate with each other in reliable manner, here, reliability is the ability to provide high delivery data ratio and send most of the messages in spite of links breaking the paths or capacity overflows caused by congested nodes.

Current security mechanism demands various resources, including energy, data memory, bandwidth channel etc. howsoever, at present, these resources are very rare in small wireless network. The most usual security approach is encryption technique which needs too many resources and as said earlier resources are limited in many cases.

On that account these networks need some particular protocols that provide initiative and self-starting behavior [14].

4. MANET Protocols

In MANET, nodes are not sure of connectivity when they move. They face considerable delay. The routing protocol use store and forward technique. A protocol is suggested about opportunistic routing with media access control in delay tolerant network. The MAC protocol utilizes characteristic of broadcasting in wireless medium and the nodes working together participate by swapping RST/CTS/DATA/ACK. The routing protocol uses store and forward technique for taking end to end reliability. The used protocol states that each node must know its velocity and position and that its movement is regular, so the ad-hoc networks use the nodes of GPS devices. The mobility-aware protocol shows the best performance than other protocols of delay tolerant (epidemic routing, geographic routing, and stray-and-wait routing) resulting small packet delay and total packet transmission [15].

Wireless sensor network (WSN) is a large network. It keeps small sensor devices which provide multicasting; a basic routing service for data transmission in activities like task assignment, code updates and targeted queries. In WSN efficient multicasting is difficult due to energy limitation. Two suggested protocols for optimization of location based multicast protocols. First, GMR [16] exploited the wireless improve the performance and multicast advantages not accurate when works for large sensor network. Second, HRPM inefficient in forwarding data packets because they are energy inefficient but they reduces the encoding time with no maintaining cost due to virtual hierarchy constriction and they use geographic hashing. HGMR (hierarchical geographic multicast routing) that joins the GMR and HRPM concepts is a multicast protocol for wireless sensor network (WSN). It is the improvement in multicast and optimization of WSN and provides energy efficiency and scalability to large network. The HGMR protocol provides healthy performance as compared with other protocols. It handles scalability and energy efficiency in multicast (WSN). The second is optimized when it transports data to nodes. The protocol that is able to rotate in every cell, several forwarding trees can take the position of Geographic multicast routing (GMR) [17].

In MANET technology various protocols are developed by programmers. MANET uses the concept of (SMP) shortest mobile path in a mobile graph for checking routing protocol. There is a comparison that the protocol uses the mean ratio of cost of route with the optimal path for same network. The protocol change resulting due to change over time. The MEAN REALVS IDEAL COSTMERIT spectrum is the representation of protocol effectiveness and it is a scalable framework instead of checking several protocols directly; compare the optimal solution of protocol as focus the comparison in same system; check in its environment one time for each protocol. The MERIT framework is good with wider generality and potential applicability as compared with routing protocol [18].

MANET is a multicasting routing protocol that is based on agent. It is the backbone

known as reliable ring. It gives robust design to link and node failure. By using computational geometry software programmer can make reliable ring with algorithms. A routing agency RRMRA improve working of multicast routing in terms of throughput, reliability, route recovery, route establishment for different mobility models. It is done with reliable ring created and managed by RRMRA agent, the result of simulation represents the working over ODMRP and ABMRS [19].

4.1. Routing in Mobile Ad-Hoc Network

In recent year, many new network routing techniques are introduced for the use of mobile ad-hoc network application. Routing in MANET can also face some critical challenges like limited range, dynamic topology and scalability. Size of routing table also affect link overhead. Many new routing techniques are developed for efficient and reliable routing. The routing protocols are divided in three parts. These parts include table driven, on demand and mixture of both of these protocol known as hybrid routing protocol.

4.1.1. Proactive Routing Protocol

Another name of this protocol is table driven routing. This protocol use one or more routing table to store the latest routing information. The information for change of the topology can propagate to all the nodes. This protocol maintains a valid route for all time for packet delivery. Because of the updating of routing table route for every other node are always available, whether they avail that or not. It uses some different method for updating the routing table. Some examples of this protocol include Dynamic Destination Sequenced Distance-Vector Routing Protocol (DSDV) Optimized Link State Routing Protocol (OLSR) and Fisheye State Routing (FSR) etc.

Destination sequenced distance-vector routing protocol (DSDV): This protocol based on "Bellman-Ford algorithm" with some improvement like as free from loops routes that provides an efficient and reliable path that lead to the final source. To reduce the overhead traffic in the network, two techniques are used for updating the whole network. First one known as a Full dump that holds all the information for updating the table and second name as incremental packet holds that information that is changed recently in last full dump. The delivery of Incremental packet is faster than full dump [20].

Optimized link state routing protocol (OLSR): OLSR is proactive in nature. This protocol depends on the link state protocol that exchanges topology change information regularly to all other nodes in network. It uses Multi-Point Relays (MPR) that helps to reduce duplication retransmission when message can be forwarded. It also reduces control overhead by using MPR. In MPR, the adjacent node known as a MPR that are selected by other nodes are transmitted data. Any other node that are MPR can translate and process packet but do not transmitted again. This will reduce the duplicate retransmission [21].

Fisheye state routing (FSR): FSR is table driven technique that depends on a "link state algorithm". It reduces the network overhead traffic and also maintains the topol-

ogy change information. In FSR each node having updated information to maintains the table. Each node also have full topology map of overall network. This information can share with local neighbors periodically. It is also scalable for wide area network but scalability can reduce the accuracy. The main problem of this technique sends link change update regularly that floods the network and also overhead traffic [22].

4.1.2. Reactive Routing Protocol

Another name of this protocol is on demand routing protocol. The reactive protocol is the technique used for discovering routes. The major aim of this protocol is to minimize the traffic load on the network. This protocol does not maintain the routing table with the change in topology. This is on demand in nature so When node needs to forward data; first it passes a message to find the route destination. The discovered route is used destination node until when it is accessible. The protocols also handle cache routes. The bandwidth of network traffic is low as compared to previous routing protocol. Dynamic Source Routing (DSR) and Ad hoc On-Demand Distance Vector routing (AODV) are two main example of on demand routing protocol [21]-[24].

Dynamic source routing (DSR): Dynamic source routing uses source routing for sending messages. In this technique sender determine the complete path of node from where the packet forwarded to destination and node also attach this route information in the header of the packet that pass from one node to the next and each node check the address of node until it reach the destination. Route maintenance and route discovery are two main feature of this protocol. In route discovery it discover the route that lead to the destination and in route maintenance whenever the topology change it detect a failure of route that lead to the destination. Whenever it indicates that source route is not present then it again discover route for propagation. The main benefit of this method is that when nodes discover routes, it first check in its cache routes and if the some authentic route are present there then the sender don't need to discover the route that is why it is helpful for those network that have low mobility.

Ad hoc on-demand distance vector routing (AODV): Ad-hoc On-Demand Distance Vector routing is the combination of both DSR and DSDV that guarantee the loop free route. Like in DSR, it use route maintenance and also route discovery for propagation and also periodic beaconing and adding sequence number from DSDV. The main difference between DSR and AODV is that in DSR each node has full routing information for network but in AODV the nodes have only the address of destination. It maintains the route whenever needed that is why it is reactive in nature. In AODV, It also add the destination sequence address to avoid looping concept when topology being change during the propagation. The main benefit of AODV is that of adaptation to active networks [20].

4.1.3. Hybrid Routing Protocol

Both previous routing protocol are useful for that scenario where the number of nodes are fewer, but when nodes increases these protocol are not efficient so in this case hybrid protocol are used that achieve higher performance in large network. This protocol

combines the feature of both above discussed routing protocol. This protocol divides the node into number of zones and clusters. The drawback of hybrid routing protocols is that nodes will consume more power and memory that have high level of information for routing. Some examples of Hybrid Routing Protocols include Zone Routing Protocol (ZRP), Hazy Sighted Link State (HSLS) protocol and Secure Routing Protocol (SRP) [21]-[23].

Zone routing protocol (ZRP): The Zone Routing Protocol (ZRP) is a hybrid in nature that contains the feature of both table driven and reactive routing protocols. In this technique the hops have predefine routing area that define the boundary of every node in proactive network connectivity. So the nodes that are in the range of routing area, their paths are directly accessible but for those hops that are outside of the area, their paths are determined reactively and these node only use reactive protocol to route which leads to the final source. The benefit of ZRP protocol is that it decreases the communication channel as compared to the table driven protocols. It also minimizes the delay of packet delivery as compared to the on demand protocols [23].

Secure routing protocol (SRP): Secure Routing Protocol is depending on "Dynamic source routing". This protocol is the combine the feature of both DSR and ZRP. It provide best routing path for the couple of nodes. In this technique the node first find the path on the network by sending some flood query on the network. It can also handle the black hole attacks.

Hazy sighted link state (HSLS) protocol: It is also a "link state protocol" that is based on the narrow propagation. HSLS does not contain the properties of on demand protocol like in ZRP but it actually shows some behavior of on demand protocol. It use best route for delivery of packet. It takes benefit of regularly improve information routing that the packet reaching the document. One important Advantage HSLS is that optimizes the overall traffic overhead [25].

5. Challenges of MANET

As soon as range of applications for mobile ad-hoc network is increase, their uses are also increased but there are some drawbacks of using the MANET technology. There are still some challenges and issues that should be concern in future research. Given below are some complexity and challenges that are face by using the MANET.

The scalability of MANET increase as it is used in secure networks so every node able to handle the overall network and fulfill their duty. In this scenario sender device is no not remain the end system. It should be act as a router or intermediate device.

Because of the rapid change in the topology of the network, the data may loss that is passing while during the topology change. Limited range, capacity and bandwidth can also the traffic.

There is no centralized mechanism for data delivery. Every mobile sends data and also act as a router to propagate message.

Every node sent update to other nodes, this will increase the network traffic overhead and that is why there may be chance for loop forming by changing the topology.

Each node act as autonomous system in network hence it is equipment for RF to re-

ceive these capabilities that Forms asymmetric link. It uses no router between these nodes for delivery of packet. Every node acts as a router in MANET [26] [27].

Quality of Service in MANET is very complex problem that could be a major concern for future researchers.

6. Conclusion

In this paper, we have presented a review of different Security issues, attacks on physical, data and network layers and also provide security solutions. Various routing protocols discussed in the paper are very helpful and effective for new researchers to identify current issues for advance research. Many new routing protocols are proposed nowadays but still there is an open research issue that which protocol shows best behavior in which situation. A lot of contribution has been made in this field but several open problems and issues need to be addressed.

Acknowledgements

We thank to our respectable teachers for giving us this chance to increase and share our knowledge. We also thank to different authors which helped us to gain information on this area.

References

[1] Abdalla, G.M., Abu-Rgheff, M.A. and Senouci, S.M. (2007) Current Trends in Vehicular ad Hoc Networks. *Ubiquitous Computing and Communication Journal*, 1-9.

[2] Abolhasan, M., Wysocki, T. and Dutkiewicz, E. (2004) A Review of Routing Protocols for Mobile Ad Hoc Networks. *Ad Hoc Networks*, **2**, 1-22. http://dx.doi.org/10.1016/S1570-8705(03)00043-X

[3] Al-Omari, S.A.K. and Sumari, P. (2010) An Overview of Mobile Ad Hoc Networks for the Existing Protocols and Applications. arXiv Preprint arXiv:1003.3565

[4] Biradar, R.C. and Manvi, S.S. (2011) Agent-Driven Backbone Ring-Based Reliable Multicast Routing in Mobile Ad Hoc Networks. *Communications, IET*, **5**, 172-189. http://dx.doi.org/10.1049/iet-com.2010.0002

[5] Chlamtac, I., Conti, M. and Liu, J.J.-N. (2003) Mobile ad Hoc Networking: Imperatives and Challenges. *Ad Hoc Networks*, **1**, 13-64. http://dx.doi.org/10.1016/S1570-8705(03)00013-1

[6] de Morais Cordeiro, C. and Agrawal, D.P. (2002) Mobile Ad Hoc Networking.

[7] Gagandeep, A. and Kumar, P. (2012) Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review. *International Journal of Engineering and Advanced Technology* (*IJEAT*), **1**, 269-275.

[8] Garg, N., Aswal, K. and Dobhal, D.C. (2012) A Review of Routing Protocols in Mobile Ad Hoc Networks. *International Journal of Information Technology*, **5**, 177-180.

[9] Ghosekar, P., Katkar, G. and Ghorpade, P. (2010) Mobile Ad Hoc Networking: Imperatives and Challenges. IJCA Special Issue on "Mobile Ad Hoc Networks", MANETs.

[10] Ghosh, C., Jana, D. and Bhaumik, B.B. (2011) Security Challenges in Reactive Mobile Ad Hoc Network. *India Conference* (*INDICON*), 2011 *Annual IEEE*, 16-18 December 2011. http://dx.doi.org/10.1109/indcon.2011.6139352

[11] Goyal, P., Parmar, V. and Rishi, R. (2011) Manet: Vulnerabilities, Challenges, Attacks, Ap-

plication. *IJCEM International Journal of Computational Engineering & Management*, **11**, 32-37.

[12] Gupta, A.K., Sadawarti, H. and Verma, A.K. (2011) A Review of Routing Protocols for Mobile Ad Hoc Networks. *SEAS Transactions on Communications*, **10**, 331-340.

[13] Haboub, R. and Ouzzif, M. (2012) Secure and Reliable Routing in Mobile Adhoc Networks. arXiv Preprint arXiv:1203.2044

[14] Yang, H., Luo, H.Y., Ye, F., Lu, S.W. and Zhang, L.X. (2004) Security in Mobile Ad Hoc Networks: Challenges and Solutions. *Wireless Communications*, **11**, 38-47. http://dx.doi.org/10.1109/MWC.2004.1269716

[15] Sun, J.-Z. (2001) Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing. *International Conferences on the Info-Tech and Info-Net*, Beijing, 29 October-1 November 2001. http://dx.doi.org/10.1109/icii.2001.983076

[16] Komninos, N., Vergados, D. and Douligeris, C. (2006) Layered Security Design for Mobile Ad Hoc Networks. *Computers & Security*, **25**, 121-130. http://dx.doi.org/10.1016/j.cose.2005.09.005

[17] Koutsonikolas, D., Das, S., Charlie, H.Y. and Stojmenovic, I. (2007) Hierarchical Geographic Multicast Routing for Wireless Sensor Networks. *International Conference on Sensor Technologies and Applications*, Valencia, 14-20 October 2007, 449-466.

[18] Li, W. and Joshi, A. (2008) Security Issues in Mobile Ad Hoc Networks: A Survey. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, 1-23.

[19] Panda, I. (2012) A Survey on Routing Protocols of Manets by Using Qos Metrics. *International Journal of Advanced Research in Computer Science and Software Engineering*, **2**, 120-129.

[20] Papadimitratos, P. and Haas, Z.J. (2003) Securing Mobile Ad Hoc Networks. CRC Press, Inc., Boca Raton.

[21] Royer, E.M. and Toh, C.-K. (1999) A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. *IEEE Personal Communications*, **6**, 46-55. http://dx.doi.org/10.1109/98.760423

[22] Ruta, M., Zacheo, G., Grieco, L., Noia, T., Boggia, G., Tinelli, E., Sciascio, E., *et al.* (2010) Semantic-Based Resource Discovery, Composition and Substitution in IEEE 802.11 Mobile Ad Hoc Networks. *Wireless Networks*, **16**, 1223-1251. http://dx.doi.org/10.1007/s11276-009-0199-5

[23] Sanchez, J.A., Ruiz, P.M. and Stojmenovic, I. (2006) GMR: Geographic Multicast Routing for Wireless Sensor Networks. 2006 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, Reston, 28 September 2006, 20-29.

[24] Sen, S., Clark, J.A. and Tapiador, J.E. (2010) Security Threats in Mobile Ad Hoc Networks. In: Al-Sakib, K.P., Ed., *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, Auerbach Publications, Boca Raton, 127-145. http://dx.doi.org/10.1201/EBK1439819197-9

[25] Singh, G. Security Threats and Maintaince in Mobile Ad Hoc Networks.

[26] Tamilarasi, M., Chandramathi, S. and Palanivelu, T. (2001) Efficient Energy Management for Mobile Ad Hoc Networks. *Ubiquitous Computing and Communication Journal*, **3**, 12-19.

[27] Hong, X.Y., Xu, K.X. and Gerla, M. (2002) Scalable Routing Protocols for Mobile Ad Hoc Networks. *IEEE Network*, **16**, 11-21. http://dx.doi.org/10.1109/MNET.2002.1020231