Comprehensive Survey of Security Issues in Routing Protocols of Manets

Nisha Yadav
M.Tech, Computer Science
Institute of Technology and Management
University
Gurgaon, Haryana

Ritu Taneja
M.Tech, Computer Science
Institute of Technology and Management
University
Gurgaon, Haryana

ABSTRACT
A network that consists of several free mobile nodes competent to move in any direction and allied from end to end through wireless links is termed as Mobile Ad hoc Networks (MANETS). MANET is basically the self-configured network supporting various modernistic applications. MANET's security is important because of wide range of multimedia programs and software running in an infrastructure-less environment, limited power and vibrant topology making it highly susceptible to severe security issues.

This paper presents a review of security threats such as dynamic and reflexive attacks, threats such as black hole and wormhole, eavesdropping, spoofing, denial of service, flooding and rushing attack etc. and summarizes the proposed solutions for handling these security liabilities by debating about various routing protocols that deliver security in MANETs.

General Terms
Threats; Security issues; Secure routing

Keywords
Ad-hoc Networks; MANETS; Routing Protocols

1. INTRODUCTION
The expression Ad hoc comes from Latin idiom, signifying "for the particular purpose". Mobile Ad-hoc system is an arrangement in that the mobile nodes such as cell phones, laptops or Personal Digital Assistants (PDAs) are coupled through wireless network devoid of an established configuration, therefore, this network is also called mobile mesh network. To send the data packets in the network, the nodes collaborate amongst each other forming a batch of mobile nodes that work individually.

There is no preset infrastructure and central management for the communication of the mobile nodes. Mobile ad hoc arrangement is a wireless set-up where communication takes place directly if the nodes are in the vicinity of each other and indirectly when there is no array of nodes within each other ultimately relying on the intermediary nodule in the latter case for communication [1]. Ultimately a wireless network is formed because of the participation of all the nodes whether directly or indirectly in the communication.

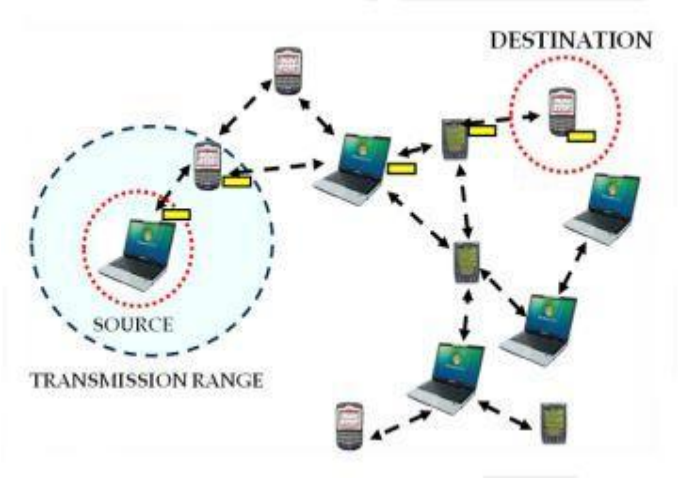

Fig 1: MANET nodes and their transmission ranges

Multi-hop routing , stoutness, low – credence terminal, self-governing terminal infrastructure-less dynamic network topologies, restricted substantial, safety hasty deployment, self operated disseminated function network topologies, energy guarded process, assuage of utilization, system scalability are some special objectives of MANET making this technology an interesting research area[2]. With the evolution, there has been growing interest in the improvement and research of MANETS. MANETs are thus, used in strategic networks, urgent situation services, location alert services and unofficial messages during meeting, sensor network, profitable and inhabitant environments i.e. in applications where the rigid infrastructure is complicate to establish and the domains that do not have incorporated arrangement[3].

This paper comprises of five major divisions. Significant security issues related to the subject of portable ad hoc system that need to be approved and addressed for providing any related solution is discussed in the section section. The following third section deals with safety measures required for secure routing in MANET while some of the common security susceptibilities and techniques to lessen the safety threats in MANETs are explained in the fourth section. And finally, conclusion of the paper is drawn in the fifth section.

2. SECURITY ISSUES IN MANETS
For the safety of communication among nodes in a potentially intimidating environment, security is a primary concern. While comparing MANETS with the wired networks, the latter one is more susceptible by protection attacks. MANET

networks are governed by physical safety measures, unbalanced topology, self-governed infrastructure, negligence and unmonitored and intimidating environment, battery subdued functions. Tribulations like packet dropping and broadcast impairment occur when the infrastructure is not fixed i.e. there is movement of nodes in the mobile ad hoc networks; ultimately cryptographic protocols are futile for this kind of flexible infrastructure where the arrangement of network keeps on changing. To avoid any dependence on centralized authority various unique ad-hoc routing protocols have been developed. MANETS are basically exceedingly dynamic and self-developing, thus, for the efficient implementation of the system in the routing procedure, the routes should be without any loop. Consumption of bandwidth, computations, unnecessary delays and power of batteries are abridged by the handling of routing protocol and loop- liberated paths simply when obligatory. For the optimal performance of the protocols unidirectional links should be used by the protocol. Spoofing is one of the attacks that MANETS are susceptible to. Various security procedures are required to warranty the preferred performance in ad hoc routing protocols.

Applying encryption and validation methods are applied to the routing protocols for improving security. The significant factor in the ad hoc steering method is service excellence. Set of rules of Ad hoc routing protocols should govern the following features such as battery power of the mobile devices should be conserved by either switching to power cutback or standby form when not to be utilized. Nodes forming the ad hoc network have very restricted assets. For initiating route discovery an alternative route is chosen when any of the link fails, so that one can be used when failed thus, the protocol should have superfluous routes. The protocol should be made defiant to recurrent topology changes by buffering multiple routes.

3. SECURITY GOALS

Investigators have measured the various security services such as accessibility, secrecy, reliability, validation and non-repudiation to protect the routing protocols in MANETs.

Despite attacks, **accessibility** warranties the survivability of the network services. Defiance of service and misconduct of node attacks leads to trouncing of availability of services and resources. To shove or conflict communication over physical canal jamming technique is employed by the intruders on MAC (medium access control) and physical layer[4]. There can be disruption on important executive services and on further services of high level as well as on network layer routing protocol on higher layers. Even in the subsistence of these attacks the services of network are available because of accessibility aspect.

Secrecy is of vital importance in tactical or premeditated military communications as this attribute ensures that there should never be disclosure of specific information to unauthorized entities. In certain situations, information about routing must also be kept secret for enemies as for locating the targets in the battleground that information can be found valuable [5].

Reliability Malevolent attacks and channel clatter are the reasons for the corruption in the message on the network [6]. Thus, a message that is on the way to the destination is never corrupted is ensured by the reliability attribute.

Intruder can achieve access to perceptive information and could pretense as a normal node without **validation** feature [7.8]. Thus, a node is enabled by validation element for ensuring the uniqueness of the peer nodule.

For revealing and seclusion of compromised nodes, non-**repudiation** plays significant role by ensuring that the message originator cannot refute that it is the authentic instigator.

The routing protocols becomes susceptible to threats such as passive eavesdropping to active attacks such as network partitioning, message littering , masquerade, message rerun, etc. by the wireless schemes in the networking environment. While active attacks are intimidation to accessibility, reliability, non-repudiation and validation; passive attacks is a menace to confidentiality. Roaming nodes with meager physical protection are quite susceptible and should be compromised in an ad hoc environment. To instigate attacks in opposition to the routing protocols, the compromised nodes can be used as preliminary points.

4. SECURITY THREATS & ITS SOLUTIONS

Smooth functioning of the network is disrupted because of the existence of susceptibilities and some impending loopholes in MANETs. Thus, there is an extensive scope for the intruders to attack because of the exploitation and attack by the malevolent and detrimental nodes. A few of the common threats in MANETs are:

4.1 Passive Attacks

These are the threats where the mugger without altering snoops the data exchanged in the network. Confidentiality is the attribute that is basically targeted by this attack. The functioning in the network system does not affect these attacks, thus, there is difficulty in the detection of this type of attack. One can determine the communication pattern and information about the network using passive attack. Passive attack espies passwords and sensitive information that can be used in setting up other types of attacks.

Eavesdropping

Mobile ad hoc networks are obtaining secret confidential information such as password, public and private keys as well as determining the location of the nodes are the primary concern for eavesdropping. By analyzing packets, transmitted data is wedged by the attacker in a particular time domain ultimately leading to detection of the destination, source, number and size transmitted time. Thus, in the process of communication efforts should be made that the private data should not be disclosed anyhow.

• Radio interface can be prevented by Spread Spectrum Communication techniques and Frequency Hopping techniques to protect the nodes from eavesdropping [9].

Traffic Analysis

Traffic analysis is entirely a reactive attack of data link layer. The rate of recurrence and the shipment of the traffic are scrutinized by means like time correlation monitor, a model like RF direction finder or software such as traffic rate analysis. Traffic analysis can expose topology behind network, about source and destination, settings, operation and functioning of the node by just requiring a wireless card working in a licentious domain.

• Traffic analysis can be avoided by either protecting wireless MAC set of rules or by supporting security of the link layer [10].

Selfishness

Selfishness is basically a threat in that the selfish nodes try to take pro of other nodes by consuming their resources unlike corrupting other nodes. These nodes save their power battery by preventing other nodes from using their resources by snubbing sent packets and using network services for their own transmission. So, this obstinate functioning of the nodes is termed as selfishness.

• Obstinate behavior of nodes is identified by an efficient scheme called TWOACK to alleviate the origin through decisive routing protocol [11].

Impersonation or Spoofing

For disrupting routing operations, forged links are advertised by the malicious node with the non-neighbors by concealing their real characteristics. In this type of attack routing packets are formed for dividing the network. While the packet is received, changes are made in the MAC or IP address of the leaving packet by the malicious node making their own identification in the network [12].

• Utilizing safe public key validation based on the trust model.

4.2 Active Attacks

Active attacks are very dangerous as there is modification and alteration of the exchange of the records by the invader in the system. This attack leads to disruption of the normal functioning of the network [13, 14]. There is an attempt to steal, modify, inject, and drop the packets by the intruders to break the protection features ultimately leading to dissemination of data files.

Jamming

In the physical layer, haphazard clatter and pulse are some of the customary forms of signal jamming leading to the troubles like no data retrieval or low data speed transmission. Signals are transmitted with the same tempo as the data is exchanged by the two communicating parties.

• One can block denial-of-service attacks by the usage of spread spectrum mechanism.

Node Isolation Attack

Node isolation is the attack that is understood by the term itself i.e. the communicating nodes are detached by not allowing to spread the link information ultimately affecting the entire communication of the network. As the nodes are made isolated and are unknown for every other node in the network, the route of the communicating nodes is not created in this attack. OLSR protocol is attacked by this attack.

• The confined component of intrusion detection for OLSR is Intrusion Detection System (IDS) leading to non-conformance valuation of the every nodule in the system that ultimately reveals the existence of threat on routing protocol [16].

Black-hole Attack

An attack where a malevolent nodule advertises having the shortest and the straight route to the destination leading to the exploitation of the routing protocol is termed as black-hole threat. Without having an active route to the destination, these nasty nodes fallaciously replies route requests thus increasing the congestion in the network because of retransmissions. The malicious node drops the packets and does not allow packets to be forwarded to the destination.

• Through the customary RREPs and distinction in successive figures to the target, the black hole threat is found that should be effectively augmented by the node of intruder for making it appear reliable to the source node in the Ad hoc On Demand Distance Vector (AODV) method [17].

Sink-hole Attack

One of the solitary of the severe threats in wireless Ad hoc system is sink-hole attack. To generate itself as explicit node wrong routing information is advertised by a compromised node to gather and attract the network traffic toward itself. In this attack, an attempt is done by the intruder to convince the adjacent nodes that an undeviating course to the target goes through it. Secret information is modified when the whole network traffic is received making it complicated by either moving the data packet or dropping them. Increasing the sequence number or decreasing the hop count such as using AODV protocol exaggerates the performance of Ad hoc system protocols.

• The very popular on demand routing protocol AODV is considered in that changes occurred is observed through the assessment by the changeable figure of nodes, interruption at the closing junctions, through sachet loss, analyzing throughput and diverse performance metrics, for e.g. PDR.

Wormhole Attack

Wormhole attack takes place in the network layer. In this attack, at one location, the packets are recorded and captured and tunneled at another location in the network leading to a high speed private connection by the intruder. There is the disruption of the routing because of the false routes created and disfigured topology when the routing control messages are tunneled again in the network [18].

• Concepts of physical and sequential packet leashes, directional antenna, connectivity based approach, transmission time based mechanism, liteworp and mobiworp, digital signature based approach, dispersion of novelty theory based approach, protocol explicit solutions, geometric analysis of multipath, graphical and topological information based approaches are the current existing solutions of Wormhole attacks.

Sleep Deprivation

The target node is persistently kept busy in this attack; therefore, this is also called as resource consumption attack. In sleep deprivation attack the network gets flooded with routing traffic through the consumption of the entire battery wealth and computing. For the consumption of the systems bandwidth and batteries wealth either unnecessary packet are forwarded to the victim node or an excessive route discovery is requested.

• Intrusion detection algorithms based on danger theory also called as DCA is used to detect consumption of resources over MANET.

Rushing Attack

The malicious node is included in the routing path in this type of attack. A request for forwarding packets towards the victim node through a discovery route towards the victim node is initiated by the intruder and assures to be the first to arrive at the surrounding nodes. Discovery route deliver hasty demand of invader to the victim node constituting of the path step all the way from attacking node. Later the requirements are unessential from the authorized nodes.

• Some of the routine mechanisms such as detecting and delegating neighbor that are secure and forwarding randomized course request protect the arrangement from rushing threat[21].

Denial of Service (DoS) Attack and Flooding

The network infrastructure is collapsed in the data link layer attacks called Denial of Service (DoS) Attack. Utilizing extra bandwidth or consuming all resources makes the services of network useless. The services are greatly degraded by transmitting unnecessary advertisements and injecting a lot of forged data to cripple the smooth functioning of the network by the intruders.

• The way the intruder degrades the performance of the networkk is considered through anonymous secure routing procedure (ASR). An effortless tempo based control packet forwarding method to mitigate malicious control packet has been developed. For alleviating tumbling of packet and sachet flooding in system, an obligation based model termed as fellowship has been proposed [22].

Table 1. Summary of the security attacks and the techniques to mitigate them in brief

Security attack	**A brief description of the Security Attack**	**Techniques proposed to mitigate the attacks**
Eavesdrop-ping	Transmitted data is lodged by the attacker in a particular time domain leading to disclosure of private data.	Use of Spread Spectrum Communication and Frequency Hopping techniques.
Traffic Analysis	Rate of recurrence and the shipment of the traffic are scrutinized.	Protecting wireless MAC set of rules or by supporting security of the link layer.
Selfishness	Nodes take pro of other nodes by consuming their resources.	TWOACK scheme is used to identify the obstinate behavior of nodes.
Spoofing	Identity and characteristics of different nodes in the network are understood by the attacker.	Utilizing safe public key validation based on the trust model.
Jamming	Leads to the troubles like no data retrieval or low data speed transmission.	Blocking denial-of-service attacks by the usage of spread spectrum mechanism.
Node Isolation Attack	Nodes are detached by not allowing spreading the link info.	Use of Intrusion Detection System (IDS)
Black-hole Attack	All the packets forwarded are dropped by the intruder.	Through the use of customary RREPs and distinction in successive figures to the target.
Sink-hole Attack	Acknowledged packets are customized or fabricated.	Usage of on demand routing protocol AODV.
Wormhole Attack	Packets are replayed from one side to the other side of the network.	Digital signature based approach, dispersion of novelty theory based approach, protocol explicit solutions, geometric analysis of multipath are used.
Sleep Deprivation	Targeted node is enforced to utilize it's vital resources.	Intrusion detection algorithms based on danger theory also called as DCA detects consumption of resources.
Rushing Attack	Malevolent node is included in the routing path of the network.	Detecting and delegating neighbor and forwarding randomized course request.

5. CONCLUSION

Unmonitored deployment and the intrinsic resources constraint nature leads to a challenge in the security of MANETs. Securities in MANET are more intricate to employ in contrast with other traditional networks reason being constrained chattels of mobile stations. So, in order to resolve t the security issues, an attempt is made to present all the related issues and techniques of security in a very much inclusive way in this paper. All the essential attributes requisite for achieving the objective of security for portable ad hoc system have been presented through this piece. By surveying safety measures threats such as active attacks and passive attacks along with their accessible modern potential solutions in the dynamic field has also been deployed and conferred. To resolve security attacks many security measures solutions have been proposed due to the advance researches made in this domain but still there has been no apposite countermeasure developed against the MANETS making it liable to security attacks. One can find solutions to the attacks discussed above and the necessities where research can be made through this paper.

6. REFERENCES

[1] Anne Marie Hegland, Eliwinjum, Stig F. Mjolsnes, Chunming Rong, Oivind Kure, And Pål Spilling, "A survey of key management in ad hoc networks", IEEE communications, 2006.

[2] Mazda Salmanian, Ming Li, 'Enabling secure and reliable policy-based routing in MANETs", IEEE Trans. 2013. M. Rajesh Babu et al., An Energy Efficient Secure Authenticated Routing Protocol for Mobile Ad hoc Networks. International Journal of Reviews in Computing, Vol. 7, Sep.2011.

[3] Neetu Singh Chouhan and Shweta Yadav "Flooding Attacks Prevention in MANET", International Journal of Computer Technology and Electronics Engineering, Vol. 1, No. 3, pp. 68-72, 2011.

[4] Robinpreet Kaur & Mritunjay Kumar Rai, A Novel Review on Routing Protocols in MANETs, Undergraduate Academic Research Journal (UARJ), ISSN : 2278 – 1129, Volume-1, Issue-1, 2012

[5] C. S. R. Murthy and B. S. Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols", New Jersey: Prentice Hall, 2004.

[6] H. Gossain, C. D. M. Cordeiro, and D. P. Agrawal, "Multicast Over Wireless Mobile Ad Hoc Networks: Present and Future Directions", IEEE Network, Vol. 17, No. 1, pp. 52-59, Jan.-Feb. 2003.

[7] P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), SanAntonio, TX, January 2002..

[8] Hubaux J.-P., Buttyan L., Capkun S., "The Quest for Security in Mobile Ad Hoc Networks", ACM Symposium on Mobile Ad hoc Networking And Computing, 2001.

[9] Monika, Mukesh Kumar, Rahul Rishi, "Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review", International Journal of Computer Applications (0975 – 8887), Volume 12– No.2, November 2010.

[10] Kashyap Balakrishnan, Jing Deng, Pramod K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks", IEEE, 2005.

[11] Amit N. Thakare et al., Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks, International Conference on Advanced Information, Networking and Applications, May. 2009.

[12] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Communications, vol. 11, pp. 38-47, Feb., 2004.

[13] Claude Crrepeau et al., A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes. IEEE Transactions on Vehicular Technology, Jan.2009

[14] B. Wu, J. Chen, J. Wu, M. Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Department of Computer Science and Engineering, Florida Atlantic university http://student.fau.edu/jchen8/web/papers/SurveyBookchapter.pdf

[15] B. Kannhavong, H. Nakayama, N.Kato, Y.Nemoto and A.Jamalipour, "Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad Hoc Networks," Proceedings of the Seventh IEEE International Symposium on Computer Networks (ISCN' 06), pp. 30-35, June 2006.

[16] S.Kurosawa, H.Nakayama, N.Kato, A.Jamalipour, and Y.Nemoto, "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," International Journal of Network Security, vol. 5, no. 3, pp. 338-346, November 2007.

[17] M.A.Gorlatova, P.C.Mason, M.Wang, L.Lamont, R. Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis," Military Communications Conference, MILCOM 2006, pp. 1-7, October 2006.

[18] Y.C.Hu, A.Perrig, and D.B.Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks," Proceedings of 22nd Annual Joint Conf. IEEE Computer and Communications Societies (Infocom'03), San Francisco, CA, vol.3, pp. 1976-1986, April 2003.

[19] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", JOURNAL OF COMPUTING, VOLUME 3, ISSUE 1, JANUARY 2011, ISSN 2151-9617.

[20] Y.C.Hu, A.Perrig and D.Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proceedings of the ACM Workshop on Wireless Security (WiSe), SanDiego, California, pp. 30-40, September 2003

[21] P.Yi, Z.Dai, S.Zhang, Y.Zhong., "A New Routing Attack in Mobile Ad Hoc Networks," International Journal of Information Technology, vol. 11, no. 2, 2005.

[22] Security issues and attackes in Mobile Ad hoc Network. http://www.slideshare.net/sunitasahu101/attacks-in-manet