A Review on Manet with Various Attacks on Routing Protocol

1Vipin Verma, 2Saurabh Sharma
Department of Computer Science Engineering
SRI SAI UNIVERSTY PALAMPUR

Abstract: **In recent years, a vast research has been seen going on in the field of Mobile Ad Hoc Networks (MANETs). Due to limited resources in MANETs, to design an efficient and reliable routing strategy is still a challenge. An intelligent routing strategy is required to efficiently use the limited resources. Also the algorithms designed for traditional wired networks such as link-state or distance vector, does not scale well in wireless environment. Routing in MANETs is a challenging task and has received a tremendous amount of attention from researchers around the world. To overcome this problem a number of routing protocols have been developed and the number is still increasing day by day. It is quite difficult to determine which protocols may perform well under a number of different network scenarios such as network size and topology etc. There are many attack in manet network which also decrease the performance of the network Main objective of writing this paper is to develop a system which having very less effect on attacks & having high network performance.**

***Index Terms*—Mobile ad hoc networks, Routing Protocols, Security.**

1. INTRODUCTION

MOBILE Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration. Therefore, MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes. Furthermore, each mobile node in MANET plays a routerrole while transmitting data over the network. In MANET all nodes are free to join and leave the network, also called open network boundary. All intermediate nodes between a source and destination take part in routing, also called hopby-hop communications. As communication media is wireless, each node will receive packets in its wireless range, either it has been packets destination or not. Due to these characteristics, each node can easily gain access to other nodes packets or inject fault packets to the network. Therefore, securing MANET against malicious behaviours and nodes, became one of the most important challenge in MANET

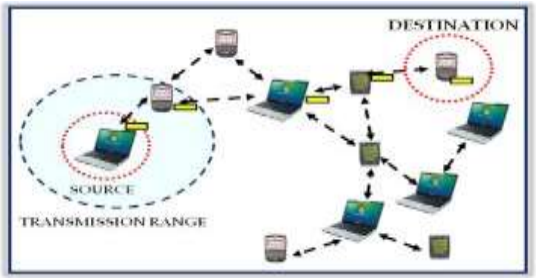

Fig 1. Mobile Ad Hoc Network

2. MANET ROUTING PRINCIPLES

The first pieces of literature we will discuss are a pair of survey papers by [1], [8], these two survey papers gather together information on the wide variety of MANET routing protocols which researchers have developed to meet the challenges of MANET routing, many of which feature different methods of managing the issues associated with mobility. [8] Performed an extensive research survey into the available routing protocols and attempted to categories them by the features they exhibit and provide details on the core protocols of each category. This is similar to work undertaken by [1] who took a similar approach in grouping routing protocols using the categories; geographical, multi-path, hierarchical, geo-cast and power aware routing protocols. The two survey papers both find that every protocol identified also fit into the core categories of; reactive, proactive or hybrid routing protocols in additional to any other characteristics they exhibit.

A. Proactive Routing

Proactive protocols rely upon maintaining routing tables of known destinations, this reduces the amount of control traffic overhead that proactive routing generates because packets are forwarded immediately using known routes, however routing tables must be kept up-to-date; this uses memory and nodes periodically send update messages to neighbors, even when no traffic is present, wasting bandwidth [10]**.** Proactive routing is unsuitable for highly dynamic networks because routing tables must be updated with each topology change, this leads to increased control message overheads which can degrade network performance at high loads [11].

B. Reactive Routing

Reactive Protocols use a route discovery process to flood\the network with route query requests when a packet needs to be routed using source routing or distance vector routing Source routing uses data packet headers containing routing information meaning nodes don't need routing tables; however this has high network overhead. Distance vector routing uses next hop and destination addresses to route packets, this requires nodes to store active routes information until no longer required or an active route timeout occurs, this prevents stale routes [10]. Flooding is a reliable method of disseminating information over the network, however it uses bandwidth and creates network overhead, reactive routing broadcasts routing requests whenever a packet needs routing, this can cause delays in packet transmission as routes are calculated, but features very little control traffic overhead and has typically lower memory usage than proactive alternatives, this increases the scalability of the protocol [1].

C. Hybrid Routing

Hybrid protocols combine features from both reactive and proactive routing protocols, typically attempting to exploit the reduced control traffic overhead from proactive systems whilst reducing the route discovery delays of reactive systems by maintaining some form of routing table [10]. The two survey papers [1], [8] successfully collect information from a wide range of literature and provide detailed and extensive reference material for attempting to deploy a MANET, both papers reach the conclusion that no single MANET routing protocol is best for every situation meaning analysis of the network and environmental requirements is essential for selecting an effective protocol. While these papers contain functionality details for many of the protocols available, performance information for the different protocols is very limited and no details of any testing methodologies is provided, because of this the validity of some claims made cannot be verified.

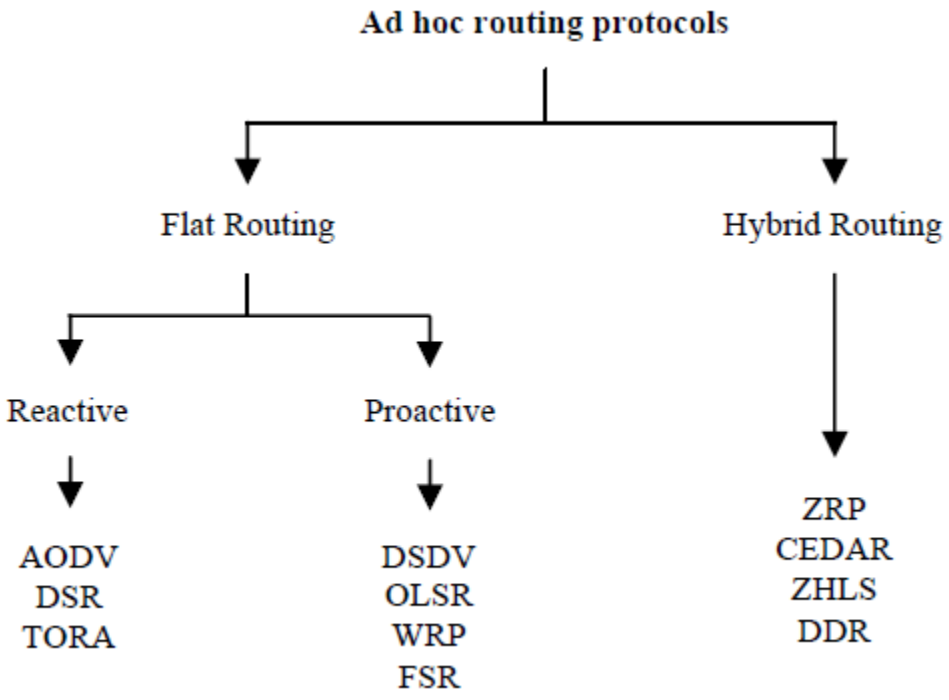

Fig 2. Manet Routing Protocol

3. Attacks

Due to special features like hop-by-hop communications, wireless media, open border and easy to setup, MANET became popular for malicious nodes. Some of the most important attacks in MANET are as follows:

3.1 Black Hole Attack: In this attack, malicious node injects fault routing information to the network and leads packets toward itself, then discards all of them [2-4]. In [5] we present a survey on black hole detection and elimination approaches. Also we presented a classification of defeating approach for this attack. Authors in [6] presented a new approach based on confirming the best path using second path. In this approach, whenever a source node receives RREP packets, it send a confirmation packet through the second best path to the destination and ask the destination whether it has a route to the RREP generator or to the Next_Hop_Node of RREP generator or not. If the destination has no route to this nodes, both RREP generator and it's Next_Hop_Node will mark as malicious nodes. Using this approach source node can detect cooperative malicious nodes. Whoever in the case of more than two cooperative malicious nodes, this approach can't detect all malicious nodes.

3.2 Worm Hole Attack: In worm hole attack, malicious node records packets at one location of the network and tunnels them to another location [7]. Fault routing information could disrupt routes in network [8]. Authors in [9] presented a way to secure MANET against this attack by using encryption and node location information. But as mentioned before, key distribution is a challenge in MANET.

3.3 Byzantine attack: In this attack, malicious node injects fault routing information to the network, in order to locate packets into a loop [10, 11]. One way to protect network against this attack is using authentication. Authors in [11] presented a mechanism to defeat against this attack using RSA authentication.

3.4 Snooping attack: The goal of this attack is accessing to other nodes packets without permission [12]. As in MANET packets transmitted hop by hop, any malicious node can capture others packets.

3.5 Routing attack: In this attack, malicious node tries to modify or delete node's routing tables [2, 3, 13]. Using this attack, malicious node destroys routing information table in ordinal nodes. Therefore, packet overhead and processing time will increase.

3.6 Resource consumption attack: In this attack, malicious node uses some ways to waste nodes or network resources [14, 15]. For instance, malicious node leads packets to a loop that consists of ordinal nodes. As a result, node's energy consumed for transmitting fault packets. In addition, congestion and packet lost probability will increase.

3.7 Session hijacking: Session hijacking is a critical error and gives an opportunity to the malicious node to behave as a legitimate system [16, 17]. Using this attack, malicious node reacts instead of true node in communications. Cryptography is one of the most efficient ways to defeat this attack.

3.8 Denial of service: In this attack, malicious node prevents other authorized nodes to access network data or services [18-19]. Using this attack, a specific node or service will be inaccessible and network resources like bandwidth will be wasted. In addition, packet delay and congestion increases.

3.9 Jamming attack: Jamming attack is a kind of DOS attack [20]. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets [21].

3.10 Impersonation Attack: Using this attack, attacker can pretend itself as another node and injects fault information to the network [22-23]. As MANET has open border and hop-by-hop communications, it's hardly vulnerable against this attack. In some cases even using authentication is useless.

3.11 Modification Attack: In this attack, malicious nodes sniff the network for a period of time. Then, explore wireless frequency and use it to modify packets [24, 25]. Man-in-the-middle is a kind of Modification attack.

3.12 Fabrication Attack: In fabrication attack, malicious node destroys routing table of nodes by injecting fault information [26-28]. Malicious node creates fault routing paths. As a result, nodes send their packets in fault routes. Therefore, network resources wasted, packet delivery rate decreased and packet lost will growth Man-in the-middle attack: In this attack, malicious node puts itself between source and destination. Then, captures all packets and drops or modifies them [29-31]. Hop by hop communications are made MANET vulnerable

against this attack. Authentication and cryptography are the most effective ways to defeat this attack.

3.13 Gray Hole Attack:
This attack is similar to black hole. In black hole, malicious node drops all packets, while in this attack; malicious node drops packets with different probabilities [32-35]. As it relays some packets, detecting this attack is more complicated than black hole and some detection approaches like sniffing or watchdog will be useless in it.

3.14 Traffic Analyze Attack:
The goal of this attack is sniffing network traffic to use them in another attack or in a specific time [34, 36]. Malicious node captures all packets to use them later. In this section we discussed security aspects in detail. Figure 2 presents a summarization of MANET's security aspect.

4. MAJOR CHALLENGES IN MANET

Regardless of the attractive applications, the features of MANET introduce several challenges that must be studied carefully before a wide commercial deployment can be expected. These include [37,38] Dynamic topologies: Nodes are free to move arbitrarily; thus, the network topology--which is typically multi hop, may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links. Routing: Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive. Multi cast routing is another challenge because the multi cast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

4.1 Device discovery- Identifying relevant newly moved in nodes and informing about their existence need dynamic update to facilitate automatic optimal route selection. Bandwidth-constrained-variable capacity links: Wireless links will continue to have significantly lower capacity than their hardwired counterparts. Power-constrained and operation: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation. For most of the light-weight mobile terminals, the communication-related functions should be optimized for lean power consumption. Conservation of power and power- aware routing must be taken into consideration.

4.2 Security and Reliability: In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to e.g. nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics introduce also reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobility-induced packet losses, and data transmission errors. Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered.

4.3 Quality of Service (QoS): Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. An adaptive QoS must be implemented over the traditional resource reservation to support the multimedia services. Inter-networking: In addition to the communication within an ad hoc network, inter-networking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management. Multicast: Multicast is desirable to support multiparty wireless communications. Since the multicast tree is no longer static, the multicast routing protocol must be able to cope with mobility including multicast membership dynamics (leave and join). IP-Layer Mobile Routing-An improved mobile routing capability at the IP layer can provide a benefit similar to the intention of the original Internet, viz. "an interoperable internetworking capability over a heterogeneous networking infrastructure". Diffusion hole problem: The nodes located on boundaries of holes may suffer from excessive energy consumption since the geographic routing tends to delivers data packets along the hole boundaries by perimeter routing if it needs to bypass the hole. This can enlarge the hole because of excessive energy consumption of the node boundaries nodes

5. CONCLUSION

Mobile Ad Hoc Network (MANET) is a kind of Ad hoc network with mobile, wireless nodes.

Due to its special characteristics like open network boundary, dynamic topology and hop-by-hop communications MANET faced with a variety of challenges. Since all nodes participate in communications and nodes are free to join and leave the network, security became the most important challenge in MANET. In this paper we study all the difficulties arise in the manet environment. There are various attack in manet which also degrade the network performance. No, security protection scheme will completely remove the effect of attack. So, we have to create a system which will increase the network performance & decrease the effect of attack. We shall create a Centralized system in manet, hope that increase the network performance & reduce the effect of attack.

REFERENCES

[1] R.Sheikh, M. S. Chande, ad D. K. Mishra, "Security issues in MANET:A review," presented at the Seventh International Conference On Wireless And Optical Communications Networks (WOCN), 2010.

[2] S.a.A.k.G, H.o.d.R.m, and S. sharma, "A Comprehensive Review of Security Issues in Manets," International Journal of Computer Applications vol. 69 2013.

[3] V.P.and R. P. Goyal, "MANET: Vulnerabilities, Challenges, Attacks, Application," IJCEM International journal of Computational Engineering & management, vol. 11, 2011.

[4] A.MISHRA, R. Jaiswal, and S. Sharma, " A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in Ad hoc Network," presented at the 3rd International Conference on Advance Computing Conference (IACC), 2013

[5] N.-W. Lo and F.-L. Liu, "A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET," in Intelligent Technologies and Engineering Systems.vol. 234, J. Juang and Y.-C. Huang, Eds., ed: Springer New York, 2013, pp. 59-65.

[6] M.A. Gorlatova, P. C. Mason, M. Wang, and L. Lamont, " Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis," Military Communications Conference, IEEE, MILCOM, 2006.

[7] S.Keer and A. Suryavanshi, "To prevent wormhole attacks using wireless protocol in MANET," presented at the nternational Conference on Computer and Communication Technology (ICCCT), 2010.

[8] Z.A.Khan and M. H. Islam, "Wormhole attack: A new detection technique," presented at the international conference on Emerging Technologies (ICET), 2012.

[9] M.Yu, M. C. Zhou, and W. Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments," IEEE Transactions on Vehicular Technology, vol. 58

[10] G.Singla, M. S. Sathisha, A. Ranjan, S. D., and P. Kumara, "Implementation of protected routing to defend byzantine attacks for MANET's," International Journal of Advanced Research in Computer Science, vol. 3, p. 109, 2012.

[11] G.Singla and P. Kaliyar, "A Secure Routing Protocol for MANETs Against Byzantine Attacks," Computer Networks & Communications (NetCom), Lecture Notes in Electrical Engineering, vol. 131, pp. 571-578, 2013.

[12] B.Kannhavong, H. Nakayama, Y. Nemoto, and N. Kato, "A survey of routing attacks in mobile ad hoc networks," Wireless Communications, IEEE Transactions, vol. 14 , pp. 429-442, 2011.

[13] L.Rajeswari, A. Prema, R. A. Xavier, and A. Kannan, "Enhanced intrusion detection techniques for mobile ad hoc networks," presented at the International Conference on Information and Communication Technology in Electrical Sciences (ICTES), 2007.

[14] A.K.Rai, R. R. Tewari, and S. K. Upadhyay, "different type of attacks on integrated MANET-internet comunication," international jornal of computer science and security (IJCSS),vol. 4.

[15] J.Y.Kim, H. K. Choi, and S. Song, "A secure and lightweight approach for routing optimization in mobile IPv6," EURASIP Journal on Wireless Communications and Networking -Special issue on wireless network security, vol. 7, 2009.

[16] Supriya and M. Khari, "Mobile Ad Hoc Netwoks Security Attacks and Secured Routing Protocols: A Survey," Advances in Computer Science and Information Technology. Networks and Communications Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 84, pp. 119-124, 2012.

[17] J.Soryal and T. Saadawi, "IEEE 802.11 Denial of Service attack detection in MANET," Wireless Telecommunications Symposium (WTS), 2012.

[18] R.H.Jhaveri, S. J. Patel, and D. C. Jinwala, "DoS Attacks in Mobile Ad Hoc Networks: A Survey," presented at the Second International Conference on Advanced Computing & Communication Technologies (ACCT), 2012

[19] J.Su and H. Liu, "Protecting Flow Design for DoS Attack and Defense at the MAC Layer in Mobile Ad Hoc Network," Applied Informatics and Communication Communications in Computer and Information Science, vol. 224, pp. 233-240, 2011.

[20] A.Hamieh and J. Ben-othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks Using Error Distribution," presented at the International Conference on Communications, ICC '09. IEEE, 2009.

[21] D.Glynos, P. Kotzanikolaou, and C. Douligeris, "Preventing impersonation attacks in MANET with multi-factor authentication," hird International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, WIOPT, 2005.

[22] C.Douligeris, P. Kotzanikolaou, and D. Glynos, "Preventing Impersonation Attacks in MANET with Multi-Factor Authentication," WIOPT '05 Proceedings of the Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2005.

[23] M.Barbeau, J. Hall, and E. Kranakis, "Detecting Impersonation Attacks in Future Wireless and Mobile Networks," Secure Mobile Ad-hoc Networks and Sensors Lecture Notes in Computer Science, vol. 4074, pp. 80-95, 2006.

[24] N.Dixit, S. Agrawal, and V. K. Singh, "A Proposed Solution for security Issues In MANETs," International Journal of Engineering Research & Technology(IJERT), vol. 2, 2013.
[25] Vaithiyanathan, S. R. Gracelin, E. N. Edna, and S. Radha, "A Novel Method for Detection and Elimination of Modification Attack and TTL Attack in NTP Based Routing Algorithm," presented at the International Conference on Recent Trends in Information, Telecommunication and Computing (ITC), 2010
[26] P.Yi, X. Jiang, and Y. Wu, "Distributed intrusion detection for mobile ad hoc networks," Journal on Systems Engineering and Electronics, IEEE, vol. 19, 2008.
[27] S.R. Afzal, S. Biswas,J. B. Koh, T. Raza, and m. authors, "RSRP: A Robust Secure Routing Protocol for Mobile Ad Hoc Networks," presented at the Wireless Communications and Networking Conference,WCNC, IEEE, 2008.International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015
[28] P.T. Tharani, K. Muthupriya, and C. Timotta, "Secured consistent network for coping up with gabrication attack in MANET," international journal of Emerging Technology and Advanced Engeineering, vol. 3, 2013.
[29] D.Sharma, P. G. Shah, and X. Huang, "Protecting from Attacking the Man-in-Middle in Wireless Sensor Networks with Elliptic Curve Cryptography Key Exchange," presented at the NSS '10 Proceedings of the Fourth International Conference on Network and System Security, 2010.
[30] K.Vishnu, "A new kind of transport layer attack in wireless Ad Hoc Networks," presented at the International Conference on Wireless Communications, Networking and Information Security (WCNIS), 2010
[31] X.Zou, A. Thukral, and B. Ramamurthy, "An Authenticated Key Agreement Protocol for Mobile Ad Hoc Networks," Mobile Ad-hoc and Sensor Networks Lecture Notes in Computer Science, vol. 4325, pp. 509-520, 2006.
[32] J.Liu, F. Fu, J. Xiao, and Y. Lu, "Secure Routing for Mobile Ad Hoc Networks," presented at the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, SNPD, 2007.
[33] J.Sen, B. Tata, M. Chandra, S. Harihara, and H. Reddy, "A mechanism for detection of gray hole attack in mobile Ad Hoc networks," presented at the 6th International Conference on Information, Communications & Signal Processing, 2007
[34] G.Usha and S. Bose, "Impact of Gray hole attack on adhoc networks," presented at the International Conference on Information Communication and Embedded Systems (ICICES), 2013
[35] G.Xiaopeng and C. Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks," presented at the IFIP International Conference on Network and Parallel Computing Workshops, NPC Workshops, 2007.
[36] C.Gray, J. Byrnes, and S. Nelakuditi, "Pair-wise Resistence to traffic Analysis in MANETs," ACM SIGMOBILE Mobile Computing and Communications Review, 2008.
[37] Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1), 2003, pp. 13–6.
[38] HaoYang, Haiyun & Fan Ye ― Security in mobile ad-hoc networks: Challenges and solutions,‖, Pg. 38-47, Vol 11, issue 1, Feb 2004.
[39] S.Shaw, K. Orea, P. Venkateswaran, and R. Nandi, " Simulation and Performance Analysis of OLSR under Identity Spoofing Attack for Mobile Ad-Hoc Networks," Computer Networks and Information Technologies Communications in Computer and Information Science,vol. 142, pp. 308-310, 2011.
[40] A.Michael and Nadeem, "Adaptive intrusion detection & prevention of denial of service attacks in MANETs," presented at the IWCMC '09 Proceedings of the International Conference on Wireless Communications and Mobile Computing, Connecting the World Wirelessly, 2009.

