ISSN No. 0976-5697

Volume 7, No. 4, July-August 2016

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Routing Attacks and their Countermeasures in MANETs: A Review

Sakshi Sachdeva
Research Scholar (M. Tech)
Department of Computer Science & Engineering,
Ambala College of Engineering and Applied Research,
Devsthali, Ambala, India

Ms. Parneet Kaur
Sr. Assistant Professor
Department of Computer Science & Engineering,
Ambala College of Engineering and Applied Research,
Devsthali, Ambala, India

Abstract: A Mobile ad hoc network is a collection of mobile devices where each device participates in routing by forwarding data to other nodes. MANETs can be employed in various situations ranging from emergency operations and disaster relief to military service and task forces, so security is an essential component for protected communication between nodes. There are a number of challenges in security design as ad hoc network is a decentralized network and vulnerable to various internal and external attacks. In this paper, we discuss about various attacks affecting normal routing procedure, their countermeasures and defense mechanisms and comparison between these defense mechanisms.

Keywords: MANET, Attacks, Security, Detection, Routing

I. INTRODUCTION

Biometrics In the past few years, wireless technology has gained precedence in the world of data communication and this has caused a proliferation of devices complying with the standards of wireless technology. In different areas like in corporate sector various computers necessitate to be connected among themselves, this can be executed either by employing infrastructured networks using base station for controlling purpose or infrastructure less networks can be used where no central administration exists.

Mobile Adhoc Networks (MANET) are the self-configuring, infrastructure less wireless ad hoc networks having the dynamic topology without any centralized administration as there is absence of any base station or access point [1]. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore acts as a router.

II. CLASSIFICATION OF ATTACKS IN MANET

Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET [2, 3]. The attacks in MANET are categorized as:

- **Passive attacks:** These attacks are launched by adversaries just to snoop the information exchanged in the network and compromise the confidentiality without causing any physical damage or disruption in the network. These are difficult to detect because the network is not affected by such attacks. E.g., Eavesdropping, traffic analysis, monitoring.
  - **Traffic Analysis and Monitoring:** It is used to identify and gain information about the communication parties and functionality which could be further exploited to launch other attacks.
  - **Eavesdropping:** It implies overhearing the communication channel by an unintended recipient without expending any extra effort. Mobile nodes in MANET share a wireless medium that utilizes RF spectrum and is broadcasting in nature so messages can be easily eavesdropped.
  - **Traffic Analysis** Traffic analysis is a passive attack used to gain information on which nodes communicate with each other and how much data is processed.

- **Active attacks:** These attacks disrupt the normal functioning and routing procedure in the wireless network. They may alter, modify, fabricate or destroy the data being exchanged in the network. Active attacks are further categorized as follows:
  - **External attacks:** These are launched out by the mobile nodes outside the range or domain of the network. They are easy to detect and can be prevented by cryptographic mechanisms. Eg spoofing, flooding attack.
  - **Internal attacks:** These are launched by the malicious nodes present within the network so difficult to detect as compared to external attacks. E.g. blackhole, wormhole, jellyfish, byzantine etc.

© 2015-19, IJARCS All Rights Reserved

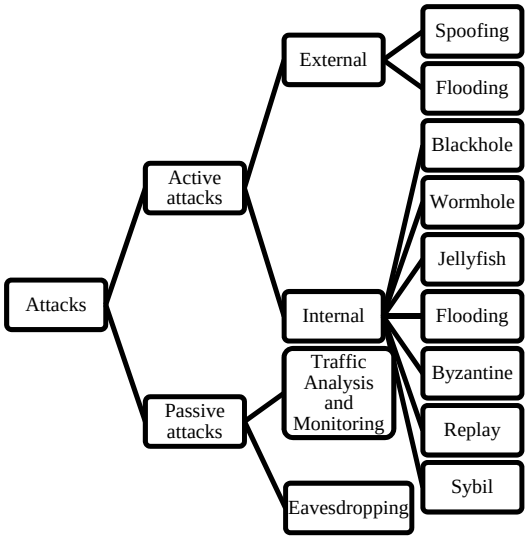

Fig. 1 Classification of attacks

III. ROUTING ATTACKS AGAINST MANET PROTOCOLS

Many routing protocols have been proposed for MANETs. These protocols fall under three main categories: proactive, reactive, and hybrid [4]. Proactive protocols maintain routes to all the nodes in the network. They incur huge processing and routing overhead as routing updates are sent periodically. E.g. DSDV, OLSR [5]. Reactive protocols are based on demand for data transmission. Routes between hosts are determined only when they are explicitly required for communication and forwarding packets. E.g. DSR, AODV, AOMDV [6]. They can significantly reduce routing overhead since they do not need to update route information periodically. Hybrid protocols combine proactive and reactive protocols to find efficient routes, without much routing overhead. E.g. ZRP. The routing protocols were developed without considering security issues. There are many security attacks in MANET that target or exploit these routing protocols and flaws in their functionalities. An attacker or malicious node can absorb network traffic, fabricate messages, inject themselves in the path between the source and destination and thus control the network traffic flow. Some of the routing attacks are discussed below:

- **Black hole Attack:** This is an internal attack in which an attacker advertises itself as having a shortest and fresh route to destination fooling all nodes around it. A malicious node first sends fake routing information, claiming that it has an optimum route and causes other nodes to route data packets through the malicious one [7]. Thereafter, malicious node drops all the received packets instead of forwarding those packets normally in the network.
- **Wormhole Attack:** In this attack, two nodes work in collusion to harm the network by tunnelling the packets received at one point to another point in the network through high speed wired or wireless links, and then replay them into the network from that point [8]. The normal routing behaviour is disrupted when routing control messages such as route request, route reply, route error messages are tunnelled. This tunnel between two colluding attackers is known as a wormhole. They are hard to detect because the path used to pass on information is usually not part of the actual wireless network.
- **Byzantine attack:** A compromised individual node, or intermediate nodes work in collusion to carry out attacks such as creating routing loops, forwarding packets through non-optimal paths or selectively dropping packets resulting in disruption of routing services within the network [9]. They are difficult to detect as network appears to be functioning normally from user point of view.
- **Replay attack:** An attacker performs replay attack by retransmitting the valid control packets repeatedly to inject the network routing traffic that has been captured previously and became invalid at present. The remaining nodes modify their routing tables and add these stale packet information which disturbs the entire network routing.
- **Flooding attack**: Malicious nodes may inject false data or control packets into the network which may loop around due to false routing information such as non-existent destination address to consume or eat the bandwidth and processing resources along the way [10]. This has an adverse effect on ad hoc networks as the mobile nodes are resource constrained in terms of battery, memory and computational power and leads to unavailability of network services to legitimate nodes.
- **Jellyfish Attack:** In this attack, the malicious node first becomes a part of the network, and then it may reorder the sequence of received packets, generate unwanted delays in packet forwarding, or drop packets [11]. This attack is similar to blackhole attack but here detection is more difficult because of tendency of attacker to behave in accordance with protocol rules. This causes the misbehaving node to yield high end-to-end delay, high jitter and significantly affects the throughput of the network.
- **Sybil Attack:** In MANET, the routing procedure is based on the nodes' unique identity or address. The malicious node exploits this requirement and illicitly generates multiple fake identities of a single node known as Sybil nodes. The malicious node can either use multiple identities to create misjudgments among the nodes or use the identity of other legitimate nodes to create a false impression of that node to launch other attacks. This results in packets to be routed towards the fake identity nodes which eventually disturbs the normal communication among the nodes and prevents fair resource allocation among the nodes in the network [12].

IV. COUNTERMEASURES AGAINST ROUTING ATTACKS

There are various security solutions proposed in the literature to combat against routing attacks and selfish behavior. These proposed solutions are either new stand-alone protocols, or an integration of security mechanism into existing routing protocols such as AODV, DSR, OLSR etc. We can categorize solutions as preventive and reactive. The conventional cryptographic mechanisms such as encryption, MAC, and digital signature constitute a preventive mechanism. Reactive mechanisms include intrusion detection systems, trust based systems, reputation, acknowledgement

© 2015-19, IJARCS All Rights Reserved

and cooperation systems provide a second line of defense against routing attacks.

Patel and Chaudhari presented a scheme based on time space key cryptography and modified hash function (mSHA-1) using pseudo random function for detecting and preventing jellyfish reordering attack [13]. The time-space cryptography provides secret keys using a time difference in the time domain using TESLA broadcast authentication protocol. Initially, all the keys are generated and stored in the key tables of every node. Each source node chooses a random key for each time period and publishes it later according to the predefined schedule. There is an overhead involved in transmission of dummy packets.

Laxmi et al. proposed a light-weight direct trust-based detection (DTD) algorithm [14] which can detect and remove a JellyFish node from an active communication route in a network. Each node uses locally calculated trust values which are collected over a time period to identify whether its neighbor node is a JF-attacker or not. Simulations were carried on EXata-Cyber and performance of proposed algorithm was evaluated in terms of network throughput, overhead incurred and end-to-end delay. The detection of JF node is possible after an attack is initiated and discovered by a neighbor throughput of a network shows slight decrease initially with increase of number of attackers.

Wazid et al. [15] proposed Cluster Based Intrusion Detection and Prevention Technique (CBIDPT) and Super Cluster Based Intrusion Detection and Prevention Technique (SCBIDPT) for detection and prevention of JF reorder attack. CBIDPT works well only when intermediate node acts maliciously whereas SCBIDPT works well in presence of malicious cluster head. Cluster head compares all sequence numbers of packets stored in its buffer to the sequence numbers of packets stored in buffer of all intermediate nodes to detect misbehaving node. The simulations are done on Opnet. The End-to-end delay increases from 0.0508 to 0.0574 sec with proposed algorithm and good put has improved significantly upto 1022.07kbps from 0kbps in presence of JF attack.

Ukey et al. proposed I-2ACK [16] for preventing routing misbehaviour and detecting malicious nodes by sending acknowledgement packets back as data packets are received and using simple rating mechanism for counting the number of data packets such that it overcomes the problem of misbehaving nodes. If data packets received are below threshold value, then a misbehaving node is detected. Simulations were performed on NS-2 and results proved that I-2ACK performed better in terms of throughput, packet delivery ratio and data packets dropped in the presence of misbehaving nodes.

Shakshuki et al proposed an intrusion detection system, namely, EAACK (Enhanced Adaptive Acknowledgment) [17] which utilizes digital signature to prevent an attacker from forging acknowledgment packets. EAACK includes three components: Acknowledge (ACK), Secure-Acknowledge (S-ACK) and Misbehaviour Report Authentication (MRA). EAACK is capable of detecting malicious nodes despite the existence of false misbehaviour report. S-ACK mode makes every three consecutive nodes to work in collusion to detect misbehaving nodes in the presence of receiver collision or limited transmission power. It assumed that nodes are connected by bi-directional links and source node and the destination node are not malicious.

Avani and Rajbir proposed a non cryptographic scheme as a countermeasure against jellyfish delay variance attack [18]. It utilizes the concept of delay threshold i.e. time interval for a node to transmit the data packet to it's upstream node for detecting malicious node and thereafter traffic is re-routed through non malicious alternate route containing non malicious MPR. The performance was analyzed on NS-3 in terms of Packet Delivery Ratio (PDR) of network with varying fraction of JF nodes and system size.

Azer et al proposed a Functional Reputation system for Ad hoc Networks (FREPAN) [19] which aims to improve the MANETS performance and mitigate selfishness and misbehaviour attacks. It consists of four modules: observer, modeler, hybrid dissemination, and decision making module. The observer module monitors the network and aggregates direct and indirect information about each node from neighbours by use of the watchdog component [20] in the promiscuous mode. The modeller module combines all the information gathered into a meaningful reputation values whereas dissemination module propagates these reputation values. The decision making module penalizes node exhibiting malicious behaviour. The simulation was done on Omnet under multiple coordinated jellyfish attacks and results obtained prove that FREPAN has improved the network's performance by increasing the average network throughput.

Table 1: Comparison of detection and preventive schemes against routing attacks in MANET

Scheme	**Based on**	**Attacks**	**Routing protocol used**	**Merits**	**Demerits**
Time Space Cryptography Hashing Solution	Time-space cryptography and modified SHA-1 (mSHA-1)	Jellyfish reordering attack	AOMDV	The congestion window decreases until the attack is detected and after that the window increases exponentially. The scheme increases goodput of the network.	There is an overhead involved in transmission of dummy packets.
CBIDPT and SCBIDPT	Intrusion Detection system	Jellyfish reordering attack	AODV	Detects and prevents JF reorder attack in both environments i.e. intra-cluster and inter-cluster and improves the goodput of the network.	These schemes introduce delay in the network.
I-2ACK	Acknowledgement	Packet dropping	DSR	I-2ACK incurs lesser routing overhead as it requires lesser	It assumed that misbehaving nodes do not send or forward false

© 2015-19, IJARCS All Rights Reserved

				number of acknowledgement packets to be transmitted.	acknowledgement packet.
EAACK	Acknowledgement (ACK), Digital signatures, S-ACK, MRA	Packet dropping attacks and false misbehavior report	AODV	It can detect misbehaving nodes even in the presence of receiver collision, false misbehavior report or limited transmission power.	More routing overhead. Need of pre-distributed keys
Non-cryptographic Detection Approach	IDS and Delay Threshold	JellyFish Delay Variance	OLSR	Proposed approach is light weight in terms of resource consumption as it does not involve expensive cryptographic operation. It is resilient against JFDV attack in MANET.	It causes increased overhead due to the innumerous attempt of re routing.
Lightweight DTD	Trust management based	Jellyfish (reordering, packet dropping and delay variance)	AODV	It identifies and removes JF nodes dynamically. The simulation results prove the correctness of proposed algorithm in terms of detection rate, end-to-end delay, network throughput and scalability as number of JF-attackers increase.	It may result in false JF-attacker detections due to improper overhearing of data packets in promiscuous mode as it does not consider in-direct observations from the neighbors.
FREPAN	Reputation based	Jellyfish attack	AODV	It avoids false accusation for benign nodes. It depends on promiscuous information collected indirectly to minimize network's traffic overhead.	There is significant average end to end delay. The nodes have to work in promiscuous mode.

V. CONCLUSION

In this paper, we have presented classification of security attacks particularly routing attacks to which MANET routing protocols are vulnerable. The paper also highlighted the solutions available in the literature for routing attacks and provided comparative analysis of the countermeasures comparing their demerits and merits. MANET security constitutes a complex and challenging niche, in which research is being carried and it will result in the discovery of new attacks as well as the development of new protocols for secure communication.

VI. REFERENCES

[1] Jhaveri, R. H., Patel S.J., and Jinwala D.C. 2012. DoS attacks in mobile ad hoc networks: A survey. In Advanced Computing & Communication Technologies (ACCT), Second International Conference on, IEEE, pp. 535-541.

[2] Bhatia T and Verma A.K. 2013. Security Issues in Manet: A Survey on Attacks and Defense Mechanisms. International Journal of Advanced Research in Computer Science and Software Engineering, 3 (6), pp. 1382-1394.

[3] Aad I., Hubaux J.P., and Knightly E.W. 2008 Impact of denial of service attacks on ad hoc networks." IEEE/ACM Transactions on Networking (TON), 16(4), pp.791-802.

[4] Bhatia T. and Verma A.K. 2015. QoS Comparison of MANET Routing Protocols. International Journal Computer Network and Information Security, 9, pp 64-73.

[5] Sharma M., Kansal M., Bhatia T. 2015. Simulation Analysis of MANET Routing Protocols under Different Mobility Models. International Journal of Wireless Communications and Network Technologies, 4(1), pp. 1-8.

[6] Bhatia T. and Verma A.K. 2013. Simulation and Comparative Analysis of Single Path and Multipath Routing Protocol for MANET. Anveshanam - The Journal of Computer Science & Applications, 2 (1), pp. 30-35.

[7] Bhatia T. and Verma A.K. 2013. Performance Evaluation of AODV under Blackhole Attack. International Journal Computer Network and Information Security, 5 (2), pp 35-44.

[8] Goyal S., Bhatia T., Verma A.K. 2015. Wormhole and Sybil Attack in WSN: A Review. INDIACOM 2015:09th INDIACOM, 2nd IEEE International Conference on Computing for Sustainable Global Development, pp. 1463-1468.

[9] Gokhale V., Ghosh S.K., and Gupta A. 2011. Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks: A Survey. Security of self-organizing networks: MANET, WSN, WMN, VANET, AS. K.Pathan, pp195-225, CRC Press, Taylor & Francis Group.

[10] Laxmi, V., Mehta, D., Gaur, M.S. and Faruki, P., 2013. Impact analysis of JellyFish attack on TCP-based mobile ad-hoc networks. InProceedings of the 6th International Conference on Security of Information and Networks (pp. 189-195). ACM.

[11] Jiang, F.C., Lin, C.H. and Wu, H.W., 2014. Lifetime elongation of ad hoc networks under flooding attack using power-saving technique. Ad Hoc Networks, 21, pp.84-96.

[12] Bhuvaneswari, R., Balamalathy, N., Premalatha, S., Manimozhi, V., Parvathi, S. and Kumaresan, A., 2015. An Improve Performance, Discovery and Interruption of Sybil Attack in MANET. Middle-East Journal of Scientific Research, 23(7), pp.1346-1352.

[13] Patel, H.P. and Chaudhari, M.B., 2013, July. A time space cryptography hashing solution for prevention Jellyfish

© 2015-19, IJARCS All Rights Reserved

reordering attack in wireless adhoc networks. In Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on (pp. 1-6). IEEE.

[14] Laxmi, V., Lal, C., Gaur, M.S. and Mehta, D., 2015. JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET. Journal of Information Security and Applications, 22, pp.99-112.

[15] Wazid, M., Katal, A. and Goudar, R.H., 2012, December. Cluster and super cluster based intrusion detection and prevention techniques for JellyFish Reorder Attack. In Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on (pp. 435-440). IEEE.

[16] Ukey, A.S.A., Chawla, M. and Singh, V.P., 2013. I-2ACK: Preventing Routing Misbehavior in Mobile Ad hoc Networks. International Journal of Computer Applications, 62(12), pp. 34-39.

[17] Shakshuki, E.M., Kang, N. and Sheltami, T.R., 2013. EAACK—a secure intrusion-detection system for MANETs. Industrial Electronics, IEEE Transactions on, 60(3), pp.1089-1098.

[18] Sharma, A. and Kaur, R., 2014, September. Non-cryptographic Detection Approach and Countermeasure for JFDV Attack. In Proceedings of the 7th International Conference on Security of Information and Networks (p. 367). ACM.

[19] Azer, M. A., & Saad, N. G. E. D. (2015). Prevention of Multiple Coordinated Jellyfish Attacks in Mobile Ad Hoc Networks. International Journal of Computer Applications, 120(20), pp. 12-20.

[20] Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000) Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 255-265). ACM.

© 2015-19, IJARCS All Rights Reserved