A Comprehensive Study on Vulnerabilities and Attacks in Multicast Routing Over Mobile Ad hoc Network

Bhawna Sharma and Rohit Vaid

Abstract MANET is an autonomous collection of mobile devices. They need the features of infrastructure-less network, flexibility, random mobility, and they do not require any base station or centralized device for the communication process. Rather than this, each device in MANET acts as a client and server. So it becomes a hot research topic among researchers. Communication between nodes is completed by intermediate nodes. Sometimes the intermediate nodes act as malicious nodes by implementing any abnormal function. So we would like to guard the traditional nodes. Therefore, we examine some routing attacks, and how they drastically affect the MANET communication process.

Keywords Network security · Ad hoc network · Denial of service · Route request · Route reply · Attacks · Secure routing protocols

1 Introduction

Mobile Ad-hoc networks (MANET) are the organizations of portable processing gadgets joined remotely with no help of fixed cooperation. There are a few attributes of MANET, which are as per the following:

- No requirement of fixed street and rail organization.
- Network of the organization is dynamic.
- Two nodes be in contact straightforwardly on the off chance that they are inside radio reach.
- Less secure than wired organization.
- MANET is an independent arrangement of portable nodes. It can work in disengagement or may have doors to and interfaces with a fixed organization.
- There are bandwidth constraints and energy constraints.
- Distributed nature of action for security, controlling, and have arrangements.

B. Sharma (✉) · R. Vaid
Department of Computer Science and Engineering,
MMEC, MM (Deemed To Be University), Mullana, Ambala, India

K. Khanna et al. (eds.), *Cyber Security and Digital Forensics*,
Lecture Notes on Data Engineering and Communications Technologies 73,
https://doi.org/10.1007/978-981-16-3961-6_22

- More adaptable than fixed network.
- High client thickness and enormous degree of client portability.
- Nodal network is irregular.

In Fig. 1, design of MANET has been appeared in which a bunch of cell phones is associated together to shape a portable impromptu organization. The gadget with high calculation capacity and more battery force can be chosen as the gathering chief, who is dependable, the general administration of gathering correspondence inside the organization.

In MANET, there are different types of routing—unicast routing and multicast routing. The unicast routing is used for one-to-one communication, whereas multicast routing is used for one-to-many communications [2]. Broadcast conveys a message to all or any hub inside the organization. Multicast conveys a message to a bunch of hubs that demonstrate revenue in accepting the message. Anycast conveys a message to anybody out of a bunch of hubs, as a rule of the one nearest to the source. Geocast conveys a message to a geological area [3] (Fig. 2).

2 Multicasting

Multicasting correspondence fills in as one basic activity to help numerous uses of mobile Ad hoc networks (MANETs) that accomplishes bunch correspondence as opposed to sets of people. Multicast steering conventions turns out to be progressively significant in MANETs since they adequately arrange a lot of nodes [4]. Moreover, it gives viable coordinating to blended media applications, for instance, video social occasions, military, and rescue errands (Fig. 3).

2.1 Routing Protocols

There are many routing protocols in MANET. At whatever point a hub needs to talk with target hub, it broadcasts its current status to neighbors. Guiding shows can be arranged into proactive, reactive, and hybrid directing show.

Fig. 1 Structure of mobile Ad hoc network [1]

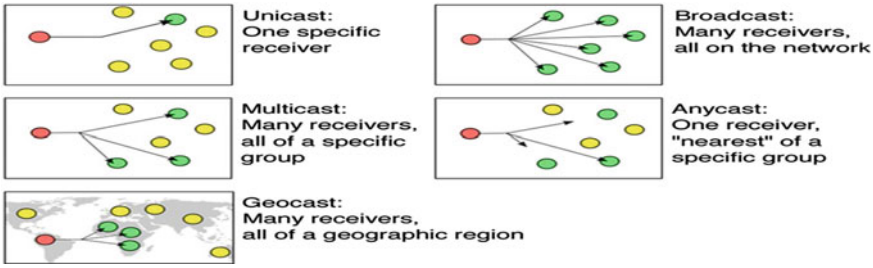

Fig. 2 Different types of routing

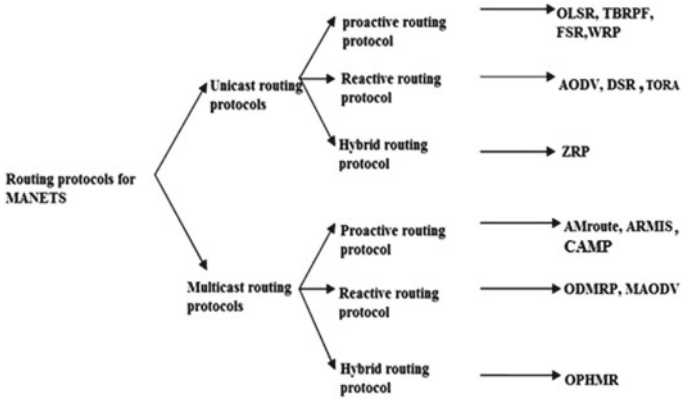

Fig. 3 Classification of routing protocols in MANET [5]

Proactive Routing Protocol:
This is a table-driven coordinating show. Each hub keeps a coordinating table which not only contains record of bordering hubs and reachable hubs, but also the amount of hops. If the size of association extends, the overhead furthermore increases which achieves decline in execution. Target sequenced distance vector (DSDV) and optimized interface state coordinating (OLSR) are proactive shows.

Reactive Routing Protocol:
This convention is likewise approached as request directing convention. At the point when a node needs to send information bundle, the responsive convention began. The preferred position of this convention is that squandered data transmission incited from consistently broadcast gets decreased. The primary weakness of this convention is that it prompts bundle misfortune. Ad hoc on-request distance vector (AODV) and dynamic source routing (DSR) are the cases of responsive directing convention. In AODV, every node records the data of next bounce in its steering table. The course revelation measure is executed at the point when the objective node cannot be reached from source node. The source node

communicates the course demand (RREQ) bundle to begin course disclosure measure. All the nodes get the RREQ packet send the course answer (RREP) parcel to the source node if the objective node data happened in their directing table. Course maintenance measure is begun when the organization geography has changed or the association has fizzled. The source node is educated by a course mistake (RRER) bundle. In DSR, nodes keep up their course store from source to objective node. Execution of DSR diminishes with the portability of organization builds, a lower bundle conveyance apportion inside the higher organization.

Hybrid Routing Protocol:
This convention contains the upsides of proactive, what is more, responsive convention. Proactive convention is utilized to accumulate the new steering data. At that point, responsive convention is utilized to keep up the steering data when geography changes. Zone routing protocol (ZRP) and temporally requested routing calculation (TORA) are the cases of crossover convention.

2.2 Security Services

MANETs are to give security administrations, for example, authentication, confidentiality, integrity, anonymity, and availability, to mobile users [5].

Confidentiality: Protection of any information from being introduced to unintended substances. In off-the-cuff associations, this is all the more difficult to achieve, considering the way that intermediate hubs get the packs for various recipients, so they can without a doubt tune in the information being coordinated.

Availability: Services should be available at whatever point required. There should be an affirmation of survivability, paying little heed to a denial of service (DOS) attack. On physical and media access control layer, the assailant can use adhering techniques to intrude with correspondence on real channel. On association layer, the attacker can upset the coordinating show. On higher layers, the attacker could chop down raised level organizations.

Authentication: Assurance that an element of concern or the cause of a correspondence is the thing that it professes to be or from. Without which, an aggressor would mimic a node in this manner, picking up unapproved admittance to asset and touchy data, and meddling with activity of different nodes.

Integrity: Message being sent is rarely adjusted.

Non-disavowal: Ensures that sending and getting gatherings can never deny truly sending or getting the message.

3 Literature Review

Jhaveri [6] proposed an MR-AODV convention which is an adjustment of R-AODV. MR-AODV not just distinguishes the dark opening and dim opening hubs, but additionally builds up free from any danger course for information transmission during the course disclosure measure.

Dhurandher et al. [7] proposes GAODV convention which is an altered AODV convention. Here, the presence of dark opening can be identified by utilizing critical control parcels CONFIRM, REPLYCONFIRM, and CHCKCNFRM. The source hub communicates RREQ message, and the middle hubs send RREP message to source, and afterwards, they unicast CONFIRM bundle to objective hub.

Karthikkannan et al. [8] proposed the grouping number distinguishing proof technique to keep away from the dark opening assaults in MANET. Here, an extraordinary grouping number will be given to every data parcel and the new bundle should have an arrangement number more noteworthy than that of pervious parcel.

In MANET, major focus was on increasing performance parameter values by developing new and updated mechanisms, and for this, several methodologies were offered. But, along with performance, security is also an important concern that must be taken care of [9]. In MANET, several attacks were found out due to which security of information can be compromised. Unauthenticated or malicious nodes are performing their attempts to be successful so that vulnerabilities can be found out in system, and accordingly, attack can also be imposed on network [10]. Each layer faces distinctive sort of assaults. Table 1 shows the normal assaults on different layers of MANETs [11].

4 Classification of Security Attacks on MANET

Making sure about MANETs is an exceptionally testing issue inferable from its existing engineering weaknesses. Assaults can be focused at steering conventions or even at security instruments conveyed in networks. Traded-off nodes can be

Table 1 Type of attacks on layers [13]

Layer	Attacks
Physical layer	Jamming, interceptions, eavesdropping
Data link layer	Traffic analysis, monitoring
Network layer	Wormhole, black hole, gray hole, message tempering, Byzantine, flooding, resource consumption, location disclosure attacks
Transport layer	Session hijacking, SYN flooding
Multiple layer	Denial of service (DoS), man-in-the-middle attack

available outside also as within the organization. Assailants can disturb typical organization steering, confine node(s), may burn through imperative assets.

4.1 Internal Attacks

This sort of assaults are started by approved (real) nodes inside an organization. An inside node may get undermined by an outer aggressor, or it might carry on egotistically to spare its assets. Inward assaults are extremely difficult to recognize.

Ex: Byzantine attacks.

4.2 External Attacks

This sort of assault is started by non-approved (non-legitimate) nodes which are not a piece of the organization. Outside bargained nodes can seriously upset organization's directing and can cause blockage in different pieces of the organization (Fig. 4).

Ex: eavesdropping.

4.3 Passive Attacks

In this assault, an aggressor just tunes in or monitors information of data that is being moved between two parties. No change and manufacture is finished. Instances of latent assaults are snooping and traffic analysis. Assailants can undoubtedly get all the data about the organization that is helpful in

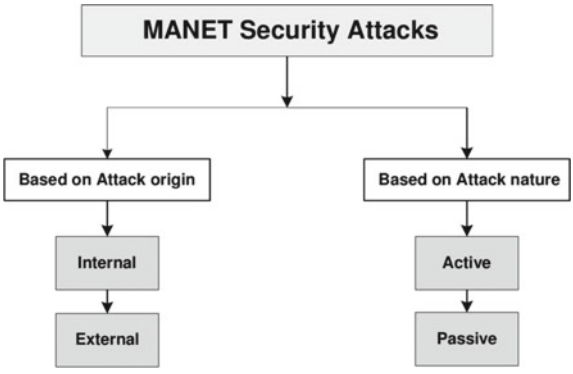

Fig. 4 Classification of security attacks in MANET

commandeering or infusing an assault in the network. It is very difficult to identify inactive assaults when contrasted with dynamic assaults [12].

Ex: eavesdropping, traffic monitoring and analysis.

4.4 Active Attacks

In this assault, an aggressor endeavors to adjust or modify the information being traded in the organization. It might disturb the ordinary working of the organizations. In dynamic assault, the interlopers can change the bundles, infuse the parcels, drop the parcels, or it can utilize the different component of the organization to dispatch the assault.

Ex: spoofing, denial of services, wormhole, black hole, sinkhole, Sybil, etc.

Wormhole Attack: In this assault, an assailant records parcels at one area in the organization and passages them to another area. This passage between two plotting assailants is alluded as wormhole. Directing can be disturbed when steering control message are burrowed [14]. Wormhole assault is utilized against on-demand routing protocol the assault could forestall the disclosure of any courses other than through the wormhole. Tunneling is used by the attacker [15].

Black-hole Attack: In this assault, a black opening is a vindictive node that erroneously answers for course demands without having a functioning course to the objective and endeavors the directing convention to promote itself as having a most brief course to objective. By promoting the most limited course, source station begins sending information through the black opening node, and it become the dynamic component in the course (Fig. 5).

Byzantine Attack: In this attack, a sabotaged temporary hub works alone, or a lot of haggled center hubs works in plan and complete attacks. These assailant hubs make controlling circles, sending groups through non-ideal ways, or explicitly dropping packs, which achieves interference or debasement of the guiding organizations.

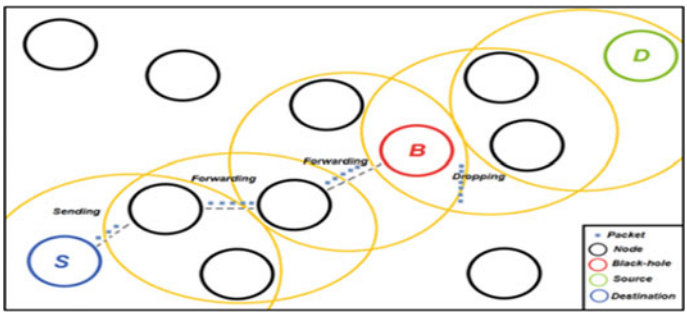

Fig. 5 Illustration of black-hole attack in MANET [16]

Traffic Monitoring and Analysis: In MANET composing, it is moreover named as location disclosure attack. In this kind of attack, the noxious hub screens, the conveyed groups, and examinations in this traffic which may reveal information, for instance, zone of sender–gatherer, sender collector pair, network topography, network coordinating structure, traffic rate, presence, zone of other genuine hubs, etc. A couple of association gadgets exist in the Web which can be used, thus, for instance, NetStumbler. Using this divulged information, other malicious hubs may similarly configure further attack circumstances in coordination. The attacker can even record, change, and retransmit changed packages to other veritable hubs remaining absolutely vague. Spillage of such information can be wrecking in security fragile conditions.

Eavesdropping: In this type of assault, the malevolent node captures the bundles sent or got, and it may uncover some classified data, for example, area of sender/beneficiary, mystery keys, passwords, and so on which might be generally left well enough alone during the correspondence between approved clients [17]. This is an aloof type of assault which owes itself because of simple tapping of remote nature of correspondence medium in MANETs.

Gray Hole Attack: In this sort of assault, a scornful node does not take an interest in course revelation instrument that is started by different nodes and is consequently not a piece of dynamic course. Such contemptuous nodes would build the course revelation disappointment and damage the general organization execution [18]. Another goal of such assailants is to moderate their energy by deciphering the message planned for them just and else they do not help out different nodes, which at last debase the presentation of the organization.

Jellyfish Attack: In this assault, the vindictive node first turns into a piece of the organization, and afterward, it might reorder the arrangement of got bundles, create undesirable postponements in bundle sending, or drop parcels [19]. This assault is like black-hole assault in any case; here, recognition is more troublesome in view of inclination of assailant to act as per convention rules. This makes the making trouble node yield very good quality to-end delay, high jitter and fundamentally influences the throughput of the organization.

Impersonation Attack: In impersonation attack, attacker node impersonates itself as authentic hub and sends bogus directing data and veils itself as sending from confided in hub [20].

Sybil Attack: Sybil attack shows itself by faking various characters by professing to involve various hubs in the association. So one single hub can anticipate the capacity of different hubs and can screen or hamper various hubs at the same time [21]. In case Sybil attack is performed over a blackmailing attack, by then degree of interference can be high. Achievement in Sybil attack depends on how the characters are created in the structure [22]. This may assist the aggressor with breaking required edge [23].

Resource Consumption Attack (RCA): Resource consumption attack (RCA) is against on-request directing convention. It is the one of DOS assaults, in which the aggressor abuses the course revelation process. During the course disclosure measure when the source node sends the RREQ parcel, at that point assailant node

kept this bundle with an alternate ID, to adjust the cycling ID of every node ceaselessly and devour its restricted energy of asset, memory, and bandwidth is appeared. The primary reason for RCA is to burn through the energy of genuine hubs and to locate the accessible connection all through [24].

Flooding Attack: Flooding assault is dispatched by flooding the organization with counterfeit RREQ's or information bundles prompting the blockage of the organization and decreases the likelihood of information transmission of the approved hubs [25]. The identification of assault is exceptionally hard, and it debilitates the organization assets (Table 2).

Table 2 Summary table

S. No.	Name of attack	Attack effect
1	Wormhole attack	• Packet drain/rope methods • MAD convention and OLSR convention • Directional reception apparatuses • Multi-dimensional scaling calculation (versatility) • Using nearby neighborhood data • DAWWSEN convention • Designing appropriate steering conventions (grouping-based and topographical steering conventions) • Leveraging worldwide information
2	Black-hole attack	• Approval and monitoring • Redundancy • Using another course • Multipath steering
3	Byzantine attack	• Prevent the route establishment • Create loops, forwards packets through non optimal paths [26]
4	Traffic monitoring and analysis	• Access control • Reduction in detected information subtleties • Distributed handling • Strong encryption methods • Sending faker bundles persistently and normal checking
5	Eavesdropping	• Access control • Reduction in detected information subtleties • Distributed preparing • Access limitation • Strong encryption procedures
6	Gray hole attack	• Cautious instruments of black-hole assault, aside from excess also, utilizing worldwide information
7	Jellyfish attack	• Compliance with all data and control protocols • Affects mainly closed-loop flows [27]
8	Impersonation attack	• Strong and legitimate verification methods • Using solid information encryption

(continued)

Table 2 (continued)

S. No.	Name of attack	Attack effect
9	Sybil attack	• Certificate authority (CA) and using personality endorsements • Limiting the quantity of hub's neighbors • Physical insurance of gadgets • Changing key consistently • Resetting gadgets and changing meeting keys (network layer) • Authentication, interface layer encryption, and worldwide shared key procedures [28]
10	Resource consumption attack	• Consumes the energy of legitimate nodes and to find the available link throughout [24]
11	Flooding attack	• Customer puzzles • AODV (Ad hoc on-request distance vector) convention • Limiting the quantity of hub's associations • Routing access restriction • Key the board

5 Conclusion

Security is the standard concern in MANETs. Because of their basic properties, for instance, dynamic topography, nonattendance of central position, confined resources and open access medium Remote exceptionally named associations are introduced to being attacked or harmed. These basic credits familiarize new troubles with interference disclosure advancement, so it is difficult to achieve security in Ad hoc network when stood out from wired organizations. In this paper, we first briefly summed up the MANET and mainstream steering conventions in it. At that point, kinds of assaults alongside a most recent review of existing arrangements are examined. Various creators have given different expert throbs for discovery and counteraction of vindictive assault in MANET, yet every methodology has its own restriction. The malignant assault is as yet a functioning research zone in MANET. In the future, assessment fuses intend to develop such a security computation, which will be presented in header of each center point that helps in acknowledgment and expectation of malicious attacks.

References

1. Chander, D., Kumar, R.: Analysis of scalable and energy aware multicast routing protocols for MANETs. Ind. J. Comput. Sci. Eng. (IJCSE) **8**(3) (2017)
2. Jain, S., Agrawal, K.: Prevention against rushing attack in mobile Ad hoc networks. Int. J. Comput. Sci. Technol. (IJCST) (2014)
3. Gridher, V., Jain, S.: Review paper on an optimized approach for attack detection and prevention in wireless sensor networks. Int. J. Comput. Sci. Technol. (IJCST) (2017)

4. Qabajeh, M.M., Abdalla, A.H., Khalifa, O., Qabajeh, L.K.: A tree-based QoS multicast routing protocol for MANETs. In: 4th International Conference on Mechatronics (ICOM) (2011)
5. Sliman, K.A., Yaklaf, A., Abdurrezagh, S.E., Ekreem, N.B., Abosdel, A.A.M.: Security routing protocols in Ad hoc networks: challenges and solutions. In: Proceedings of the International Conference on Recent Advances in Electrical Systems, Tunisia (2016)
6. Jhaveri, R.H.: MR-AODV: a solution to mitigate blackhole and grayhole attacks in AODV based MANETs. In: 2012 Third International Conference on Advanced Computing & Communication Technologies, pp. 254–260. IEEE (2012) (978–0–7695–4941)
7. Dhurandher, S.K., Woungang, I., Mathur, R., Khurana, P.: GAODV: a modified AODV against single and collaborative black hole attacks in MANETs. In: 2013 27th International Conference on Advanced Information Networking and Applications Workshops, pp. 357–362. IEEE (2013) (978–0–7695–4952)
8. Karthikkannan, P., Lavanya Priya, K.P.: Reduction of Delays in Reactive Routing Protocol for Unobservable Mobile Ad-Hoc Networks. IEEE (2013)
9. Kumar, A.: Security attacks in MANET—a review. In: IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing (2011)
10. Kumar, A., Singh, J.: Security attacks in mobile Ad hoc networks (MANET): a literature survey. Int. J. Comput. Appl. **122**(20), 31–35 (2015)
11. Mohammad, S.N.: Security attacks in MANETS (survey prospective). Int. J. Eng. Adv. Technol. (IJEAT) **6**(3) (2017). ISSN: 2249–8958
12. Dobhal, N., Pundir, D.: An investigative survey of different security attacks in MANETs. Int. J. Comput. Appl. (0975–8887) **126**(1) (2015)
13. Goyal, M., Poonia, S.K., Goyal, D.: Attacks finding and prevention techniques in MANET: a survey. Adv. Wirel. Mobile Commun. **10**(5), 1185–1195 (2017). ISSN 0973–6972
14. Rajkumar, K., Prasanna, S.: Complete analysis of various attacks in MANET. Int. J. Pure Appl. Math. **119**(15), 1721–1727 (2018)
15. Majumder, S., Bhattacharyya, D.: Mitigating wormhole attack in MANET using absolute deviation statistical approach. In: 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), pp. 317–320. IEEE (2018, January)
16. Yasin, A., Abu Zant, M.: Detecting and isolating black-hole attacks in MANET using timer based baited technique. In: Hindawi Wireless Communications and Mobile Computing Volume 2018, Article ID 9812135
17. Goyal, U., Gupta, M., Kaur, K.: Meliorated detection mechanism for the detection of physical jamming attacks under AODV and DSR protocols in MANETs. IJAIEM **3**(10) (2014)
18. Alkatheiri, M.S., Liu, J., Sangi, A.R.: AODV routing protocol under several routing attacks in MANETs. IEEE (2011) 978–1–61284–307–0/11
19. Sachdeva, S., Parneet Kaur, M.: Routing attacks and their countermeasures in MANETs: a review. Int. J. Adv. Res. Comput. Sci. **7**(4) (2016)
20. Latha, R., Sasikala, S.: A survey of routing attacks in Manet. In: Proceedings of the UGC Sponsored National Conference on Advanced Networking and Applications, 27th March 2015
21. Singh, R., Singh, J.: A novel Sybil attack detection technique for wireless sensor networks. IEEE J. Sel. Areas Commun. **10**, 185–202 (2017)
22. Saha, H.N., Bhattacharjee, D.: Different Types of Attacks in Mobile Ad hoc Network: Prevention and Mitigation Techniques. https://arxiv.org/ftp/arxiv/papers/1111/1111.4090.pdf
23. Rajakumar, P., Prasanna, V.T., Pitchaikkannu, A.: Security attacks and detection schemes in MANET. In: 2014 International Conference on Electronics and Communication Systems (ICECS), pp. 1–6. IEEE (2014, February)
24. Jain, S., Agrawal, K.: The impact of resource consumption attack on signal-stability based adapting routing protocol in MANET. In: International Conference on Recent Developments in Science, Engineering and Technology (IJST) (2016)
25. Nithya, S., Prema, S., Sindhu, G.: Security issues & challenging attributes in mobile ad-hoc networks. Int. Res. J. Eng. Technol. (IRJET) **03**(01), 1083–1087 (2016)

26. Manohar, B., Kumar, M.: Review on Byzantine attack in MANET and solution to avoid. Int. Res. J. Eng. Technol. (IRJET) **6**(1) (2019). e-ISSN: 2395–0056
27. Kaur, M., Rani, M., Nayyar, A.: A comprehensive study of jelly fish attack in mobile Ad hoc networks. Int. J. Comput. Sci. Mob. Comput. **3**(4), 199–203 (2014). ISSN 2320–088X
28. Newsome, J., Shi, E., Song, D., Perrig, A.: The Sybil attack in sensor networks: analysis & defenses. Cent. Comput. Commun. Secur. (2004)