Educational Administration: Theory and Practice
2024,30(4), 2656-2665
ISSN:2148-2403
https://kuey.net/

Research Article

Security Breaches Of Mobile Ad-Hoc Networks (MANET) - A Review

Kashyap Joshi[1], Kapil Kumar[2*]

[1,2*] Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat (India)

***Corresponding Author:** Dr Kapil Kumar,
*Associate Professor, Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat (India) E-mail: kkforensic@gmail.com Research Schola, Cyber Security and Forensic Science. Department of Biochemistry and Forensic Science, Gujarat University, Ahmedabad, Gujarat (India).

Citation: Kashyap Joshi (2024), Security Breaches Of Mobile Ad-Hoc Networks (MANET) - A Review *Educational Administration: Theory And Practice*, *30*(4), 2656-2665
Doi: 10.53555/kuey.v30i4.1912

ARTICLE INFO

ABSTRACT

Security is an essential part of any network, wired or wireless. Attackers can combine active and passive methods to penetrate otherwise undetectable routing in message and data packets, making any connection between mobile nodes in an unfamiliar environment extremely vulnerable. In this piece, we focus on the most pressing security threats facing mobile ad hoc networks. Due of its lack of protection against malicious actors, MANET can be accessed by anyone. A major MANET objective is the development of a fool proof security system capable of protecting the network against a wide range of routing assaults, even in the presence of malicious nodes. However, these approaches are flawed due to the limited resources of MANETs, such as battery life and network bandwidth. A mobile ad hoc network can operate in isolation from or in tandem with a traditional wired network. The adaptability and self-organization of MANETs are both their greatest strength and their greatest security vulnerability. This book discusses both active and passive routing attacks, such as black holes, spoofing, wormholes, and floods. Passive assaults are also discussed, such as traffic monitoring, traffic analysis, and eavesdropping.

Keywords: MANET, DOS, AODV, Data Traffic, Attacks, Security, Vulnerability.

Content:

i. Traffic Monitoring
ii. Eavesdropping
iii. Traffic Analysis
iv. Sync Flooding

- Security Challenges in MANET

i. Availability
ii. Confidentiality
iii. Integrity
iv. Authentication
v. Non-Repudiation
vi. Privacy

- Routing Security in Ad hoc Networks
- Routing Authentication

i. New key agreement scenario
ii. Two obvious problems
iii. Password based Authenticated Key Exchange

- Comparison of Secure Protocols
- Conclusion

Background:

In mobile ad hoc networks, nodes are free to move about and form their own networks. The MANET self-configures, meaning that nodes can join or depart at any time. Data is transmitted from one node to the next until it reaches its final destination, a process known as "node discovery". All of the nodes act as a relay station for information. Since MANET is adaptable, it can be used by anyone-even malicious nodes that steal information or launch DDoS attacks. As the separation between hosts increases, more energy must be put into making the Bluetooth or 802.11 (Wi-Fi) connection. That's why it's inefficient and perhaps dangerous to communicate directly between two hosts: it eats up a lot of energy and disrupts other signals. By linking two hosts through other network hosts, multi-hop transmission can circumvent this routing problem. The most reliable sources of routing information for a given destination should be prioritized by a router, and users should be able to rank their importance. A router's job is to eliminate unnecessary routes. Routers can't share routing information automatically if they don't use, believe, or trust it. Distributing routing data from a third party requires great caution and perhaps even some obsessiveness on the part of routers. [1]

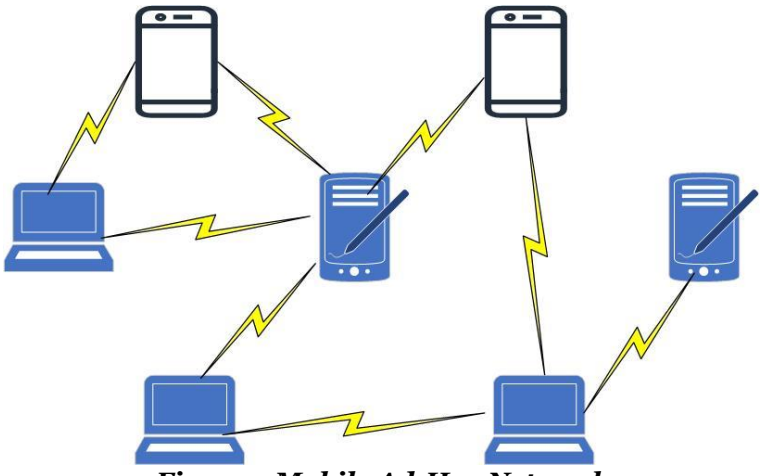

Figure 1 Mobile Ad-Hoc Network

Figure 1 shows wirelessly connected mobile ad hoc network nodes that forward and receive data. This article examines ad hoc network assaults and cryptographic key establishment methods. We discuss secure ad hoc routing protocol research and routing issues.

The Role of Routing Protocols in Ad Hoc Networks:

This section will cover various strategies used to address routing and security issues in ad hoc networks.

Routing Protocols:

There are greater routing issues in mobile ad hoc networks than in wired ones. In order to overcome the limitations of ad hoc networks, many popular protocols were created. Most routing protocols accommodate ad hoc network traits via source-initiated on-demand or table-driven architecture. Routing information on how each node is connected to all other nodes is continuously updated by table-driven ad hoc routing protocols.

Active protocols routinely refresh the network topology so that all nodes can see it. In contrast to table-driven protocols, source-initiated on-demand routing occurs only when needed. Only when the source node actually requires a route does it set one up. "The discovery of a route begins at the source node. Information is provided in chunks after a route has been discovered. Routing upkeep is essential to keeping a route operational.
The various routing strategies are shown in Table 1 according to the reaction time, bandwidth, and energy requirements of the relevant parameters.

.

Classification of Routing Protocols:

Parameter	Network	Protocols	Examples
Response Time & Bandwidth	Ad hoc	Proactive Protocols	Destination-sequenced Distance-Vector [2] [3] [4] (DSDV)
			Optimized Link- State Routing [5] (OLSR)
			Landmark Ad hoc Routing [6] [7] [8] (LANMAR)
		Reactive Protocols	Ad Hoc On-Demand Distance-Vector (AODV) [2] [3]
			Dynamic Source Routing [9] [10] [11] [12] [13] (DSR)
			Cluster-based (or hierarchical) Routing [14] [15] [16]
			Geography-based Routing [17] [18] [19]
			Location Aided Routing [20] [21] [22] [23] (LAR)
		Hybrid Protocols	Zone Routing Protocol [24] [25] [26] (ZRP)
			Zone-based Hierarchical Link State Routing Protocol [27] (ZHLS)

Table 1 Classification of Routing Protocols

Security Measures in Ad-Hoc Network:

Ad hoc networks are especially vulnerable to link attacks including passive eavesdropping, active impersonation, message replay, and message distortion because of their reliance on wireless links. If an enemy were able to eavesdrop, they might learn some crucial secrets. Deleting messages, injecting fake messages, impersonating nodes, etc. are all examples of active attacks that pose a danger to availability, integrity, authentication, and non-repudiation. Free-roaming nodes without adequate physical defenses are vulnerable to attack in a dangerous environment. That's why it's important to think about malicious assaults coming from both inside and outside the network. These methods are inherently unsafe. [28]

Vulnerability of Channels: Messages on a wireless network can be intercepted and modified by an attacker without direct access to the network's infrastructure.

Vulnerability of Nodes: Attackers can take control of network nodes since they are often not in secure rooms.

Absence of Infrastructure: The requisite infrastructure is unnecessary for ad hoc networks to function. There is no longer a need for security measures dependent on servers or certification authorities.

Dynamically Changing Topology: Due to the dynamic topology of mobile ad hoc networks, sophisticated routing protocols fraught with security concerns are required. Attacked nodes often report incorrect routes, making it difficult to identify topological shifts. To improve the chances of survival Decentralizing ad hoc networks can make them less vulnerable to attacks. The topology of ad hoc networks is dynamic and therefore constantly evolving. When vulnerable nodes are identified, the trust relationships between them shift. Security at scale needs to be adaptable.

Ad-Hoc Network Attacks:

Multiple security flaws have been identified in mobile ad hoc networks. In many ways, MANET assaults are unique. Most attacks from MANETs are both proactive and reactive. The most common kinds of attacks in these areas are detailed below. [29] [30] [31] [32]

Passive Attacks:

Passive attacks are no match for MANETs. Data in a secure network can be stolen by passive assaults. Data can be stolen via passive assaults by monitoring traffic and listening in. Because these assaults don't affect network functionality, they're tough to publicize. Data in a network is encrypted to thwart these kinds of assaults. [33] [34]

Active Attacks:

Networks are significantly harmed by active attacks. The attacker is purposefully interfering with network node communication. Criminals are aided in their abuse of network privileges by these attacks, which lead to bottlenecks, DoS attacks, control packet manipulation, and other problems. Multiple safeguards are in place to stop such attacks. Examining Some Assaults, Both Direct and Indirect. [34] [35]

Types of Active Attacks:

Black Hole Attack: A zero-metric advertisement is broadcast by the attacker to nearby targets. The bad node deceives other nodes into thinking it is the optimal path to their destination. This rogue node receives the route reply and promptly responds with an extremely brief one. The malicious node quickly interferes with network communications. Assaults on the network layer. [36] [37] [38]

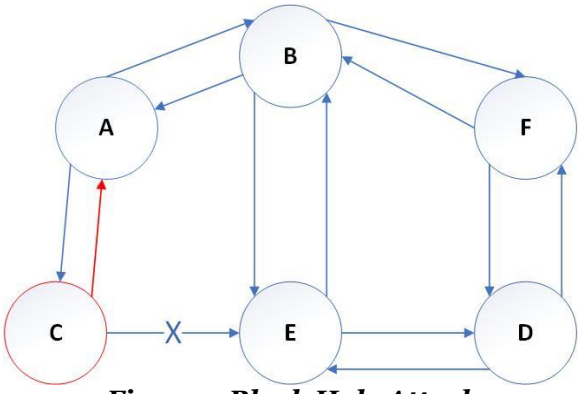

Figure 2 Black Hole Attack

Worm Hole Attack: A network tunnel is created for the purpose of this attack. Infected nodes can be used as a "tunnel" for data to be sent to other malicious actors. A wormhole was created by these malicious nodes. MANET routing is vulnerable to wormhole attacks. Without the wormhole, this assault prevents any routes from being discovered by DSR, AODV, etc. There is a hole-wearing assault on the network layer. There are primarily three types of wormhole attacks. [39] [40] [41] [42]

(i) Open wormhole: The source transmits data packets to a wormhole, which tunnels them to the other wormhole, which transfers them to the destination. Disregarded nodes don't exchange data.
(ii) Half-open wormhole: The source sends data packets directly to the destination through a wormhole.
(iii) Closed worm hole: Since data packets travel directly from source to destination, they are fictitious neighbours.

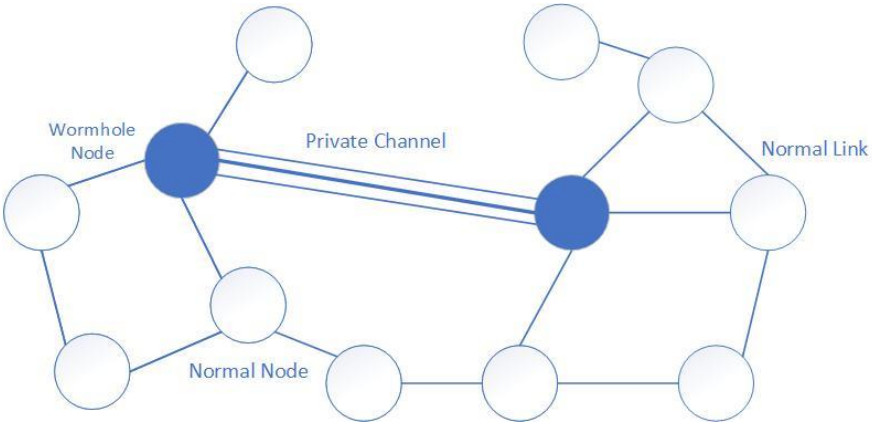

Figure 3 Worm Hole Attack

Gray Hole Attack: This vulnerability causes problems with routing algorithms and interrupts transmissions. In a two-stage process. Node marketing is the starting point because it lays out the steps needed to reach the end result. Packets having a certain match are intercepted by the node in the second step. [43] [44] [45] [46]

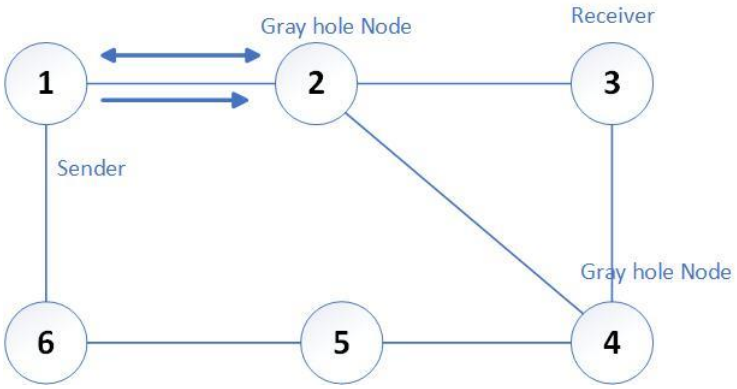

Figure 4 Gray Hole Attack

Byzantine Attack: A group of nodes inside a network can create up routing loops to deliver data packets on non-optimal routes or arbitrarily delete packets to disrupt routing services. [47] [48] [49] [50]

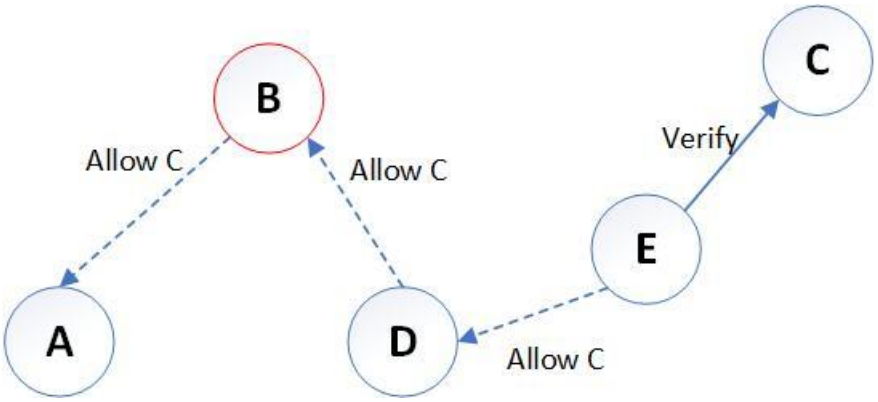

Figure 5 Byzantine Attack

Sink Hole Attack: The attacker establishes a sink node to ingest all adjacent nodes' data. This attacking node attempts seduction. This node gets lots of traffic. It also listens to neighbouring node data. [51] [52] [53]

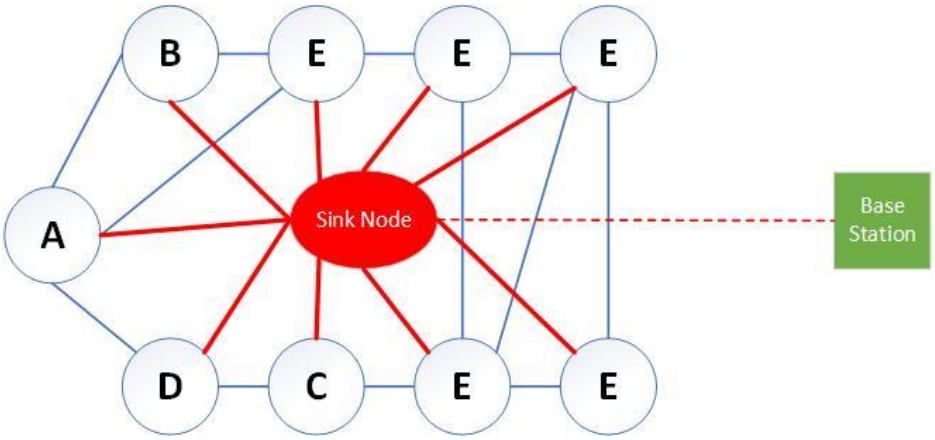

Figure 6 Sink Hole Attack

Denial of service (DoS) Attack: This exploit disables routing services for nodes. This attack disrupts network activities, including security threats, seamlessly. [54]
Jamming: The invader checks the transmission frequency in jamming. The attacker jams the network by sending a signal on an inspected frequency to block useful transmissions. These attacks are physical. [55] [56]

Types of Passive Attacks:
Traffic Monitoring: Traffic monitoring attackers use data and traffic trends. Traffic patterns reveal network topology to the attacker. Network traffic analysis may reveal the following legitimate information.
1. Node location
2. The topology of the network
3. Every node's role
4. Information about the source and destination nodes

Eavesdropping: Eavesdropping is listening to private conversations without permission. This attack involves conversation spoofing or accidental data collection. It disrupts transmission by listening in and inserting falsified messages into the network. [38] This attack steals sensitive data, such as private and public keys. These attacks are physical.
Traffic Analysis: Traffic analysis inspects every node for useful data. Traffic patterns help the attacker identify the network.
Sync Flooding: DoS attack sync flooding. Sync flooding requires many TCP connections with nodes. This attack limits valid nodes. Transport layer attacks are similar.
Security Challenges in MANET:
Multiple security issues have been carefully considered in MANET. [57] Here is a list of these difficulties:

- Availability
- Confidentiality
- Integrity
- Authentication
- Non-Repudiation

- Anonymity
- Authorization

Availability: It shows that authentic users can get helpful materials as needed. User accesses data and services. It protects networks against DoS attacks.
Confidentiality: Confidentiality assures authorization because only authorised users can access genuine information. To maintain data privacy, we must restrict access to actual information to privileged users. [39]
Integrity: Message integrity can only be changed by an authorised user. Integrity ensures message identity during transmission. Two approaches can compromise integrity:
1. Replication
2. Modification of messages

Unauthorized users changing messages, removing data streams, or needlessly copying data compromise integrity.
Authentication: Authentication ensures that nodes only reply to trusted network messages. To prevent security breaches, each data stream sender must be verified.
Non-Repudiation: Non-Repudiation assures the message's source and recipient and requires the sender to not dispute the transmission whenever a node is recognised or inspected.
Privacy: To protect valid information from unlawful disclosure, privacy is upheld.

Routing Security in Ad hoc Networks

However, while current ad hoc routing techniques can adapt to topology shifts, they provide no defenses against hackers. Neither the most frequent security threats nor secure routing instructions can be determined by a single protocol. Another potential security hole in a network is the router, which must broadcast topology information in order to construct paths between nodes. The introduction of erroneous routing information from outside the network, the re-playing of previously used routing information, the distorting of routing information, an excess of retransmissions, and inefficient routing all contribute to a network becoming overloaded. Internally damaged nodes are more challenging to diagnose and repair. By signing it with their own private keys, hackers can render routing information meaningless. The dynamic nature of Ad hoc networks makes it impossible to identify and disconnect infected nodes based on routing information alone. Ad hoc routing techniques allow for the dynamic upkeep of routing information. The fraudulent routing information that is obtained from nodes is just as out of date. If there are enough reliable nodes, the routing protocol can pick and choose among several different, possibly disconnected paths to avoid any vulnerable nodes. The routing protocol should use the backup route if the active route is unsuccessful. [58]

Routing Authentication

Due to the dearth of infrastructure, route discovery in ad hoc networks must rely on authentication of routing. That's why a route answer from a node has to make sense. Thus, authentication between ad hoc network nodes is necessary. Protocol applications are discussed here.

i) **New key agreement scenario**: Think of a spontaneous get-together where everyone brings their laptop and sets up a wireless network. Despite their mutual trust, they are unable to share a secret password. They'd rather not have their private chats overheard in public. This situation is vulnerable to assault by anyone who can listen in on, alter, or inject communications, or make it appear as though they originated from within the room. The most straightforward solution to this common Ad hoc network problem is location-based key agreement, which involves first mapping locations to names before resorting to identity-based key agreement". IP addresses can be written down and handed out on paper if desired. Key agreement based on certificates can be used. Using their IP address and key, these public key certificates can confirm the identity of a participant.

ii) **Two obvious problems:** a) It's not clear whether or not the participant's certification has been revoked. b) There may be multiple certification tiers for participants, but these tiers are unrelated. One easy solution. Because ad hoc networks lack infrastructure, it is hard for reliable third parties to pinpoint exactly where a player is. The session key is negotiated on a private, wired network only the people in the room have access to, before switching to the public, wireless network..

iii) **Password based Authenticated Key Exchange:** To preserve the group's tacit understanding, a new password is selected and distributed electronically. A long random password can be used to build up security associations, although this method is not as user-friendly. User-friendly as they are, phrases written in natural language are nonetheless susceptible to being defined incorrectly by a dictionary. Create a secure session key using a vulnerable shared secret. This procedure need to have:

Secrecy: Only participants who know the shared, weak password should learn the session key.

Perfect Forward Secrecy: Ensures that a later-successful attacker who compromises one participant cannot understand the session key from earlier protocol iterations.
Contributory Key Agreement: Every player contributes to the final session key in contributory key agreement.
Tolerance to Disruption Attempts: Weak attackers can just insert messages sent by other players without changing or removing them, but strong attackers can jam radio channels and other forms of communication. Diffie-Hellman key exchange for secure passwords.

Comparison of Secure Protocols

The three tables that follow this one compare different methods of making ad hoc networks secure. Safeguards are outlined in Table 2. better method compares in terms of different types of attacks. While RAP is not prevented by ARAN, replay attacks are. Solution criteria and operating characteristics are listed in Table 3. How can we describe the ad hoc protocols used in the secure routing protocol implemented in protocols that guarantee privacy and data integrity?
To prevent infinite loops, adopt a protocol with a count that can never go to infinity. Many different metrics are used by routing algorithms to determine the best route. Modern routing algorithms use a number of factors to determine the best path to take. Controls encompassed Finding a connection between two nodes with manageable communication costs is the goal. Multiple factors, including path length, influence reliability, delay, bandwidth, and load.
Optimizing the quickest route Input/Output Channel Using solely efficient symmetric cryptography, Adriane, a novel ad hoc network routing system, safeguards users against both single compromised nodes and active attackers. Using the DSR protocol, Adriane calculates routes between nodes on the fly. Instead of randomly encrypting the protocol, we meticulously rethought how each communication in the protocol would be processed. To protect various routing protocols, we built robust, all-encompassing security measures. Timed Efficient Stream Loss-tolerant Authentication (TESLA) can handle packet loss, can scale to a large number of receivers, and have a minimal communication and processing overhead.

Attack	***Protocol***						
	ARAN	**SRP**	**SEAD**	**ARIADEAN**	**SAODV**	**SLSP**	**OSRP**
Location Disclosure	No	No	No	No	No	No	No
Black- Hole	No	No	No	No	No	No	Yes
Re play	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Worm hole	No	No	No	No	No	No	No
Black mail	NA	NA	NA	NA	NA	NA	NA
Denial of Services (DoS)	No	Yes	Yes	Yes	No	Yes	No
Routing table Position	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rushing attacks	Yes	No	Yes	Yes	No	No	No

Table 2 Defence Against Different Types of Attack

TESLA works because the transmitter and receiver are only loosely synchronized in terms of time. Specifications for the TESLA broadcast authentication protocol: Minimal computation is needed for authenticated data production and verification. Reduced sender and receiver buffering thanks to efficient communication enables fast packet authentication, resistance to packet loss, and scalability to a large number of receivers. Security-Aware By incorporating safety measures into the routing process, Ad hoc Routing (SAR). With SAR, ad hoc routing protocols can use adaptable security as a performance indicator. "The AODV or DSR protocol is our foundation. In the original protocol, a node would send a packet called a Route Request (or RREQ) to its neighbors.

RECOMMENDED SOLUTION	**ROUTING STRATEGY**	**FREE LOOPING**	**TRAFFIC MATRIC**	**SHORTEST PATH**	**REPLY TO ROUTE REQUESTS**	**REQUIREMENTS**
ARAN	On-demand	Yes	None	Optional	No	Online reputable certification authority.
SAR	On-demand	Depends on the selected security requirements	A Security requirement	No	No	Mechanism for key distribution or secret sharing.
SRP	On-demand	Yes	Distance	No	Optional	A security association exists between each source and destination node.
SEAD	Table-driven	Yes	Distance	No	No	Clock synchronization
ARIADNE	On-demand	Yes	Distance	No	No	An online key distribution center distributes TESLA keys to participating nodes.

Table 3 Operational Requirement and Parameter of the Proposed Solution

Conclusion:

I have provided a high-level overview of the state of security in an Ad-Hoc network environment. Ad-hoc routing in wireless ad-hoc networks and key management were discussed. Ad hoc networking is still a growing field of research, as evidenced by both the problems that have arisen and the new ways in which they have been addressed". The mechanisms for managing keys remain prohibitively expensive and vulnerable to attack. Multiple routing protocols have been proposed for use in ad hoc networks. There is a pressing need to fortify and fortify these networks so that they can meet the stringent standards of these systems. These networks are projected to gain popularity due to their versatility, ease of use, and quick deployment times. Ad hoc network studies can now readily accommodate these stringent programmatic requirements.

References

1. Junhai, L., Liu, X., & Danxia, Y. (2008). Research on multicast routing protocols for mobile ad-hoc networks. Computer Networks, 52(5), 988-997.
2. Mohapatra, S., & Kanungo, P. (2012). Performance analysis of AODV, DSR, OLSR and DSDV routing protocols using NS2 Simulator. Procedia Engineering, 30, 69-76.
3. Chavan, A. A., Kurule, D. S., & Dere, P. U. (2016). Performance analysis of AODV and DSDV routing protocol in MANET and modifications in AODV against black hole attack. Procedia Computer Science, 79, 835-844.
4. Govindasamy, J., & Punniakody, S. (2018). A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. Journal of Electrical Systems and Information Technology, 5(3), 735-744.
5. Abdalla, A. M., Saroit, I. A., Kotb, A., & Afsari, A. H. (2011). Misbehavior nodes detection and isolation for MANETs OLSR protocol. Procedia Computer Science, 3, 115-121.
6. Gerla, M., Hong, X., & Pei, G. (2000, November). Landmark routing for large ad hoc wireless networks. In Globecom'00-IEEE. Global Telecommunications Conference. Conference Record (Cat. No. 00CH37137) (Vol. 3, pp. 1702-1706). IEEE.
7. Gerla, M., Hong, X., & Pei, G. (2000, November). Landmark routing for large ad hoc wireless networks. In Globecom'00-IEEE. Global Telecommunications Conference. Conference Record (Cat. No. 00CH37137) (Vol. 3, pp. 1702-1706). IEEE.
8. Abolhasan, M., Wysocki, T., & Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. Ad hoc networks, 2(1), 1-22.
9. Tarique, M., & Tepe, K. E. (2009). Minimum energy hierarchical dynamic source routing for mobile ad hoc networks. Ad Hoc Networks, 7(6), 1125-1135.
10. Boukerche, A., Oliveira, H. A., Nakamura, E. F., & Loureiro, A. A. (2008). Vehicular ad hoc networks: A new challenge for localization-based systems. Computer communications, 31(12), 2838-2849.
11. Muñoz, J. L., Esparza, O., Aguilar, M., Carrascal, V., & Forné, J. (2010). RDSR-V. Reliable Dynamic Source Routing for video-streaming over mobile ad hoc networks. Computer Networks, 54(1), 79-96.
12. Alamri, J., Al-Johani, A. S., & Ata, K. I. (2020). Performance Evaluation of Two Mobile Ad-hoc Network Routing Protocols: Ad-hoc On-Demand Distance Vector Dynamic Source Routing. International Journal of Advanced Science and Technology, 29(5), 9915-9920.
13. Kim, J., & Tsudik, G. (2009). SRDP: Secure route discovery for dynamic source routing in MANETs. Ad Hoc Networks, 7(6), 1097-1109.
14. Huang, J., Ruan, D., & Meng, W. (2018). An annulus sector grid aided energy-efficient multi-hop routing protocol for wireless sensor networks. Computer Networks, 147, 38-48.
15. Wahid, I., Ikram, A. A., Ahmad, M., Ali, S., & Ali, A. (2018). State of the art routing protocols in VANETs: A review. Procedia computer science, 130, 689-694.
16. Dutta, N., Sarma, H. K. D., & Polkowski, Z. (2018). Cluster based routing in cognitive radio adhoc networks: Reconnoitering SINR and ETT impact on clustering. Computer Communications, 115, 10-20
17. Singh, S. P., & Sharma, S. C. (2015). A survey on cluster based routing protocols in wireless sensor networks. Procedia computer science, 45, 687-695.
18. Yan, S. H. I., JIN, X. Y., & CHEN, S. Z. (2011). AGP: an anchor-geography based routing protocol with mobility prediction for VANET in city scenarios. The Journal of China Universities of Posts and Telecommunications, 18, 112-117.
19. Boussoufa-Lahlah, S., Semchedine, F., & Bouallouche-Medjkoune, L. (2018). Geographic routing protocols for Vehicular Ad hoc NETworks (VANETs): A survey. Vehicular Communications, 11, 20-31.
20. Radwan, A. A., Mahmoud, T. M., & Houssein, E. H. (2011). Evaluation comparison of some ad hoc networks routing protocols. Egyptian Informatics Journal, 12(2), 95-106.
21. Füßler, H., Widmer, J., Käsemann, M., Mauve, M., & Hartenstein, H. (2003). Contention-based forwarding for mobile ad hoc networks. Ad Hoc Networks, 1(4), 351-369.

22. Yuan, B., & Huibing, Z. (2017). Location aided probabilistic broadcast algorithm for mobile Ad-hoc network routing. The Journal of China Universities of Posts and Telecommunications, 24(2), 66-71.
23. Chatterjee, S., & Das, S. (2015). Ant colony optimization based enhanced dynamic source routing algorithm for mobile Ad-hoc network. Information sciences, 295, 67-90.
24. Yang, C. C., & Tseng, L. P. (2007). Fisheye zone routing protocol: A multi-level zone routing protocol for mobile ad hoc networks. Computer Communications, 30(2), 261-268.
25. Saini, T. K., & Sharma, S. C. (2019). Prominent unicast routing protocols for Mobile Ad hoc Networks: Criterion, classification, and key attributes. Ad Hoc Networks, 89, 58-77.
26. Yang, C. C., & Tseng, L. P. (2007). Fisheye zone routing protocol: A multi-level zone routing protocol for mobile ad hoc networks. Computer Communications, 30(2), 261-268.
27. Alotaibi, E., & Mukherjee, B. (2012). A survey on routing algorithms for wireless ad-hoc and mesh networks. Computer networks, 56(2), 940-965.
28. Nguyen, H. L., & Nguyen, U. T. (2008). A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Networks, 6(1), 32-46.
29. Nguyen, H. L., & Nguyen, U. T. (2008). A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Networks, 6(1), 32-46.
30. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2-3), 293-315.
31. Aluvala, S., Sekhar, K. R., & Vodnala, D. (2016). An empirical study of routing attacks in mobile ad-hoc networks. Procedia Computer Science, 92, 554-561.
32. Nguyen, H. L., & Nguyen, U. T. (2008). A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Networks, 6(1), 32-46.
33. Joshi, P. (2011). Security issues in routing protocols in MANETs at network layer. Procedia Computer Science, 3, 954-960.
34. Joshi, P. (2011). Security issues in routing protocols in MANETs at network layer. Procedia Computer Science, 3, 954-960.
35. Soni, M. R., Dahiya, A. K., & Verma, M. S. (2016). Security issues and attacks in mobile ad hoc networks. International Journal of Engineering Research and Technology.
36. Moudni, H., Er-rouidi, M., Mouncif, H., & El Hadadi, B. (2019). Black hole attack detection using fuzzy based intrusion detection systems in MANET. Procedia Computer Science, 151, 1176-1181
37. Hammamouche, A., Omar, M., Djebari, N., & Tari, A. (2018). Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET. Journal of information security and applications, 43, 12-20.
38. Imran, M., Khan, F. A., Jamal, T., & Durad, M. H. (2015). Analysis of detection features for wormhole attacks in MANETs. Procedia Computer Science, 56, 384-390.
39. Jhaveri, R. H., Patel, A. D., Parmar, J. D., & Shah, B. I. (2010). MANET routing protocols and wormhole attack against AODV. International Journal of Computer Science and Network Security, 10(4), 12-18.
40. Tiruvakadu, D. S. K., & Pallapa, V. (2018). Confirmation of wormhole attack in MANETs using honeypot. Computers & Security, 76, 32-49.
41. Govindasamy, J., & Punniakody, S. (2018). A comparative study of reactive, proactive and hybrid routing protocol in wireless sensor network under wormhole attack. Journal of Electrical Systems and Information Technology, 5(3), 735-744.
42. Wei, C., Xiang, L., Yuebin, B., & Xiaopeng, G. (2007, August). A new solution for resisting gray hole attack in mobile ad-hoc networks. In 2007 Second International Conference on Communications and Networking in China (pp. 366-370). IEEE.
43. Mohanapriya, M., & Krishnamurthi, I. (2014). Modified DSR protocol for detection and removal of selective black hole attack in MANET. Computers & Electrical Engineering, 40(2), 530-538.
44. Kumar, V., & Kumar, R. (2015). An adaptive approach for detection of blackhole attack in mobile ad hoc network. Procedia Computer Science, 48, 472-479.
45. Su, M. Y. (2011). Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Computer Communications, 34(1), 107-117.
46. Wang, N. C., & Chang, S. W. (2005). A reliable on-demand routing protocol for mobile ad hoc networks with mobility prediction. Computer Communications, 29(1), 123-135.
47. Mohanapriya, M., & Krishnamurthi, I. (2014). Modified DSR protocol for detection and removal of selective black hole attack in MANET. Computers & Electrical Engineering, 40(2), 530-538.
48. Mazhar, N., & Farooq, M. (2011). A hybrid artificial immune system (AIS) model for power aware secure Mobile Ad Hoc Networks (MANETs) routing protocols. Applied Soft Computing, 11(8), 5695-5714.
49. Awerbuch, B., Curtmola, R., Holmer, D., Nita-Rotaru, C., & Rubens, H. (2008). ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks. ACM Transactions on Information and System Security (TISSEC), 10(4), 1-35.
50. Goyal, P., Batra, S., & Singh, A. (2010). A literature review of security attack in mobile ad-hoc networks. International Journal of Computer Applications, 9(12), 11-15.

51. Zhang, F. J., Zhai, L. D., Yang, J. C., & Cui, X. (2014). Sinkhole attack detection based on redundancy mechanism in wireless sensor networks. Procedia computer science, 31, 711-720.
52. Stafrace, S. K., & Antonopoulos, N. (2010). Military tactics in agent-based sinkhole attack detection for wireless ad hoc networks. Computer Communications, 33(5), 619-638. .
53. Gagandeep, A., & Kumar, P. (2012). Analysis of different security attacks in MANETs on protocol stack A-review. International Journal of Engineering and Advanced Technology (IJEAT), 1(5), 269-75.
54. El Houssaini, M. A., Aaroud, A., El Hore, A., & Ben-Othman, J. (2016). Detection of jamming attacks in mobile Ad Hoc Networks using statistical process control. Procedia Computer Science, 83, 26-33.
55. Kim, J., Biswas, P. K., Bohacek, S., Mackey, S. J., Samoohi, S., & Patel, M. P. (2021). Advanced protocols for the mitigation of friendly jamming in mobile ad-hoc networks. Journal of Network and Computer Applications, 181, 103037.
56. Ponsam, J. G., & Srinivasan, R. (2014). A survey on MANET security challenges, attacks and its countermeasures. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 3(1), 274-279.
57. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2-3), 293-315.
58. Qiu, T., Chen, N., Li, K., Qiao, D., & Fu, Z. (2017). Heterogeneous ad hoc networks: Architectures, advances and challenges. Ad Hoc Networks, 55, 143-152.
59. Gambhir, S., & Sharma, S. (2013, February). PPN: Prime product number based malicious node detection scheme for MANETs. In 2013 3rd IEEE International Advance Computing Conference (IACC) (pp. 335-340). IEEE.
60. Sarika, S., Pravin, A., Vijayakumar, A., & Selvamani, K. (2016). Security issues in mobile ad hoc networks. Procedia Computer Science, 92, 329-335.
61. Nguyen, H. L., & Nguyen, U. T. (2008). A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Networks, 6(1), 32-46.
62. Lee, S. B., Ahn, G. S., Zhang, X., & Campbell, A. T. (2000). INSIGNIA: An IP-based quality of service framework for mobile ad hoc networks. Journal of Parallel and distributed Computing, 60(4), 374-406.
63. Joshi, P. (2011). Security issues in routing protocols in MANETs at network layer. Procedia Computer Science, 3, 954-960.
64. Bai, F., Sadagopan, N., & Helmy, A. (2003). The IMPORTANT framework for analyzing the Impact of Mobility on Performance Of RouTing protocols for Adhoc NeTworks. Ad hoc networks, 1(4), 383-403.
65. Nguyen, H. L., & Nguyen, U. T. (2008). A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Networks, 6(1), 32-46.
66. Nguyen, H. L., & Nguyen, U. T. (2008). A study of different types of attacks on multicast in mobile ad hoc networks. Ad Hoc Networks, 6(1), 32-46.
67. Khanna, N., & Sachdeva, M. (2019). A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs. Computer Science Review, 32, 24-44.
68. Mokhtar, B., & Azab, M. (2015). Survey on security issues in vehicular ad hoc networks. Alexandria engineering journal, 54(4), 1115-1126.