International Journal of Applied Science and Engineering
Citation: *IJASE*: **11**(02): 107-112, December 2022
DOI: 10.30954/2322-0465.3.2022.4

IJASE
INTERNATIONAL JOURNAL OF APPLIED SCIENCE AND ENGINEERING

Review Paper

COMPUTER SCIENCE

Design and Analysis of Security Protocol in Mobile *Ad-hoc* Networks

Milindkumar Vinayakrao Sarode

Head of Department, Computer Engineering, Government Polytechnic, Nagpur, India

Corresponding author: mvsarode2013@gmail.com

Received: 21 Sept., 2022 **Revised:** 26 Nov., 2022 **Accepted:** 03 Dec., 2022

ABSTRACT

These days' security protocols are a crucial element to provide security services for mobile *ad-hoc* networks. These services contain data confidentiality, message integrity, subscriber authentication, automated payment system, etc. In this research paper I proposed, design of effective security protocols. Some security protocols are presented and some collective attacks against security protocols are conferred. The susceptibilities that lead to the attacks are analyzed and guidelines for effective security protocol design are proposed.

Keywords: Security protocols, protocol attacks, *Ad-hoc* Networks, Challenger

In this paper I introduce security protocols and the most common attacks in the security protocols. There are many protocols that exist that help in the security of data over the internet such as Secure Socket Layer (SSL), Transport Layer Security (TLS). Sequence of operations that ensure protection of data. Used with a communications protocol, it provides secure delivery of data between two parties. The term generally refers to a suite of components that work in tandem (see below). For example, the 802.11i standard provides these functions for wireless LANs. SSL and TLS are separate protocols; however, TLS is a successor version of SSL. After SSL v3.0, TLS came into focus, and at present, TLS 1.3 is in practice by certificate authorities.

The wireless communication companies have many segments such as cellular telephone, satellite based communication, local area networks (LANs) and worldwide interoperability for microwave oven access (WiMAX). The de facto acquisition of the IEEE 802.11 standard[1] has fuelled the evolution of WLANs by ensuring interoperability of wireless transmission technologies among various vendors thereby supporting the technology's market penetration. This standard defines the specifications of the first two layers of the Open System Interconnection (OSI) communications protocol stack[2] and operates in the unallocated ISM electromagnetic spectrum frequency band. Depending on the underlying configuration, the IEEE 802.11 standard[1] defines two major wireless networks for WLANs i.e. infrastructure based and infrastructure less based networks.

How to cite this article: Sarode, M.V. (2022). Design and Analysis of Security Protocol in Mobile *Ad-hoc* Networks. *IJASE.,* **10**(02): 107-112.

Source of Support: None; **Conflict of Interest:** None

MANETs are autonomous and adaptive in that the topology of a formed network cans alteration on-the-fly without the interference of a system administrator[4,11]. Although MANETs share many of the properties of the traditional wired networks, they possess certain unique characteristics which derive from the inherent nature of their wireless communication medium and the distributed function of their medium access mechanisms. The issues involved may be categorized as follows.

Wireless Channel: The wireless communication medium (or channel) is vulnerable to a assortment obstacles, for example, way misfortune impedance and blockage[12,13]. These factors restrict the range, data rate and reliability of the wireless transmission. A signal is considered successfully received at a node if the measured signal to interference and noise ratio (SINR) is large enough to be decoded. Normally, the transmitted signal has an immediate way part between the transmitter and receiver[12]. Different parts of the transmitted signal alluded to as multi-way component are signals reflected, diffracted or scattered by nature, and touch base at the receiver shifted in amplitude, frequency and phase as for the immediate way component[12]. Estimation of path loss is difficult in outlining and deploying of 802.11 networks, since it quantifies the impacts of the landscape and the carrier frequency used on signal propagation. Several path loss models have been suggested for 802.11 networks[4,15]. The free space propagation model is the least difficult path loss model which expects the presence of a direct-path signal between the transmitter and the receiver, with no environmental attenuation of multi-path components. Another well-known wireless signal propagation model is the two-ray ground model[16] which accept that the signal reaches the receiver through two ways, one a viewable pathway path, and another the path through which the reflected or refracted and scattered wave is received. One of the significant issues that torment radio frequency networks is multi-path fading[4]. This alludes to the fast changes in signal strength when received at the recipient, and it is typically caused by propagation mechanisms, quite, reflection, refraction or diffraction of the transmitted signal. For instance, most mobile nodes working on 802.11 are outfitted with omni-directional antennas which emanate radio frequency power in all ways. Signals spread outwards from the transmitting antenna and are reflected, refracted or diffracted by obstacles within the transmission radius[14,15]. The signal received at the receiver is the sum of all the different components. The combined signal at the receiver may give a net superposition of 0 (i.e. if different components of the signal arrived 1800 out of phase), in which case the receiver would not be able to decode the signal.

OBJECTIVE OF THE PAPER

The principle objectives of this research work are:

- To provide the overview on data security of for Mobile ad hoc network.
- To Analyze secure network protocol in *Ad-hoc* mobile networks.

Network Security Protocols

Untruthful principal (or attacker, intruder, spy, enemy, adversary, etc.) tries to manipulate the protocol to accomplish a biased advantage. The main difficulty in the development of effective security protocols is to address the vast opportunities of a challenger to gain information. In disparity to communications protocols, the main issues are reachability of all legal conditions and escaping of infinite loops, security protocol verification deals with the gain of information by an challenger.

The challenger can be either passive or active. An active adversary is more dangerous than a passive observer.

Basic protocols permit communication agents to authenticate each other, to establish fresh session keys for confidential communication, and to ensure the authenticity of data and services. Erection on such basic communication protocols, more advanced services like non-repudiation, fairness, etc. are accomplished.

Attacks on Network Security Protocols

An attack on a network security protocol is a sequence of actions performed by an attacker, by means of any hardware or software tool, in order to disrupt protocol goals. The attacker is a dishonest participant.

A network security protocol should impose the data exchange between honest participants, while the dishonest ones should denies any benefit of it. However, network security protocols have some weaknesses which feat the conceptual structure of the protocols and are independent on the network systems. These weaknesses make them vulnerable to a range of attacks such as freshness, parallel session and type-flaw attacks.

A freshness attack is common attacks on authentication and key-formation protocols. If the messages swapped in an authentication protocol do not carry suitable freshness identifiers, then an intruder can get himself authenticated by replaying messages copied from a legitimate authentication session.

A parallel session attack requires the parallel execution of multiple protocol runs, where the intruder uses messages from reference to synthesize messages in the attack session.

A multiplicity attack is a parallel session attack that can occur when the principals disagree on the number of runs they think they have successfully completed with each other. A type flaw attack involves the replacement of a message component with another message of a different type by the intruder.

Analysis of Routing Protocols in Mobile *Ad-hoc* Networks

The following parameters have been analyzed:

1. **Packet Delivery Fraction**: is the ratio of received packets by constant bit rate at the destination over sent packets by constant bit rate Source. This metric actually expresses the reliability level of the protocol. It gives the loss rate in transport protocol, which affects the maximum throughput the ad hoc network can support.
2. **Average End-to-End Delay:** It is the delay that could be caused by buffering during route discovery, queuing delays at interface queues, retransmission delays at the Medium Access Control, and transfer times.
3. **Throughput:** Throughput refers to how much data can be transferred from one location to another in a particular amount of time.

Proposed Guidelines for Network Security Protocol Design in *Ad-hoc* Mobile Networks

(a) Freshness Attack Guidelines in Mobile *Ad-hoc* Networks

The cryptographic contents transmitted in a response of the protocol does not contain any fresh component for the recipient; so a freshness attack can be equine. An alternate solution to prevent the freshness attack is the addition of a timestamp to the encrypted message of the protocol. This solution also avoids the attack, as the recipient can check that the timestamp is recent. If an intruder attempts to replay message from a previous run, the recipient will be able to detect this replay as the timestamp will be expired. Applying Parallel Session Attack Guidelines in Mobile *Ad-hoc* Networks.

To confirm the applicability of the projected guidelines, for the case when the key used for the encryption of the messages belonging to a challenge-response handshake of a protocol is public. In the case when the key used for the encryption is private, CCITT X.509 protocol can be considered.

CONCLUSION

This paper introduced security protocols and common attacks in Mobile *Ad-hoc* Networks that deed weaknesses in the design of security protocols. Two dissimilar types of attack - freshness and parallel session attacks - that deed known weaknesses in the design of these protocols. The causes of these weaknesses that made the protocols susceptible to the attacks are analyzed. Based on this analysis guidelines for security protocol design in *Ad-hoc* Mobile Networks are presented. Protocols that follow to these guidelines will be secure against the existing types of attack.

The applicability of the proposed guidelines for security protocol design in Mobile *Ad-hoc* Networks is demonstrated well. Amenability with these guidelines successfully detects and avoids the freshness and parallel session attacks in Mobile *Ad-hoc* Networks.

REFERENCES

1. Kumar, R., Tripathi, S. and Agrawal, R. 2018. "A secure handshaking AODV routing protocol (SHS-AODV)", 2018 4th International Conference on Recent Advances in Information Technology (RAIT), Pages: 1 - 5.

2. Chintalapalli, R.M. and Ananthula, V.R. 2018. "M-LionWhale: multi-objective optimization model for secure routing in mobile ad-hoc network", *IET Communications,* **12**(12): 1406 – 1415.

3. Hurley-Smith, D., Wetherall, J. and Adekunle, A. 2017. "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks", *IEEE Transactions on Mobile Computing,* **16**(10): 2927 - 2940.

4. Yadav, S., Trivedi, M.C., Singh, V.K. and Kolhe, M.L. 2017. "Securing AODV routing protocol against black hole attack in MANET using outlier detection scheme", 2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON), Pages: 1 - 4.

5. Brill, C. and Nash, T. 2017. "A comparative analysis of MANET routing protocols through simulation",

2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), Pages: 244 - 247.

6. Bhargavi, V.S., Seetha, M. and Viswanadharaju, S. 2016. "A trust based secure routing scheme for MANETS", 2016 6th International Conference - Cloud System and Big Data Engineering (Confluence), Pages: 565 - 570.

7. Kundu, A., Misra, R. and Kar, A. 2016. "On demand secure routing protocol using Convex-Hull & K-mean approach in MANET", 2016 IEEE 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), Pages: 1 - 5.

8. Moudni, H., Er-rouidi, M., Mouncif, H. and Hadadi, B.E. 2016. "Secure routing protocols for mobile ad hoc networks", 2016 International Conference on Information Technology for Organizations Development (IT4OD), Pages: 1 - 7.

9. Yadav, P. and Hussain, M. 2017. "A secure AODV routing protocol with node authentication", 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), **1**: 489 - 493.

10. Singh, U., Samvatsar, M., Sharma, A. and Jain, A.K. 2016. "Detection and avoidance of unified attacks on MANET using trusted secure AODV routing protocol", 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Pages:1- 6.

11. Sharma, S. 2017. "A secure reputation based architecture for MANET routing", 2017 4th International Conference on Electronics and Communication Systems (ICECS), Pages: 106 - 110.

12. Saurabh, V.K., Sharma, R., Itare, R. and Singh, U. 2017. "Cluster-based technique for detection and prevention of black-hole attack in MANETs", 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), **2**: 489 - 494.

13. Gadekar, S. and Kadam, S. 2017. "Secure optimized link state routing (OLSR) protocol against node isolation attack", 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Pages: 684 - 687

14. Sultana, J. and Ahmed, T. 2017. "Securing AOMDV protocol in mobile *adhoc* network with elliptic curve cryptography", 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE), Pages: 539 - 543.

15. Nguyen, D.Q. and Toulgoat, M. 2016. Louise Lamont, "Impact of trust-based security association and mobility on the delay metric in MANET", *Journal of Communications and Networks,* **18**(1): 105 - 111.

16. Singh, S., Dutta, S.C. and Singh, D.K. 2012. "A study on Recent Research Trends in MANET". *International Journal of Research and Reviews in Computer Science (IJRRCS),* **3**(3): 1654–1658.

17. Yih-Chun Hu, 2006. "Wormhole Attacks in Wireless Networks", *IEEE Journal on Selected Areas in Communications,* **24**(2): 370 – 380.

18. Dazhi, S. and Zhenfu, C. 2008. New cryptanalysis paradigm on a nonce-based mutual authentication scheme. *International Journal of Network Security,* **6**(1): 116-120.

19. Burrows, M., Abadi, M. and Needham, R. 1990. A logic of authentication. *ACM Transactions on Computer Systems TOCS*, **8**(1): 18-36.

20. Gavin, L. 1995. "An attack on the Needham-Schroeder public key authentication protocol", *Information Processing Letters,* **56**(3): 131–136.

21. Dojen, R., Lasc, I. and Coffey, T. 2008. "Establishing and Fixing a Freshness Flaw in a Key-Distribution and Authentication Protocol", *In:* IEEE International Conference on Intelligent Computer Communication and Processing, August 2008, pp. 185-192.

22. Satyanarayanan, M. 1989. Integrating security in a large distributed system. *ACM Transactions on Computer Systems,* **7**(3): 247–280.

23. Dolev, D. and Yao, A.C. 1983. On the Security of Public Key Protocols. *IEEE. T. on Information Theory*, **29**(2): 198-208.

24. Denning, D. and Sacco, G. 1981. "Timestamps in key distributed protocols", *Communication of the ACM,* **24**(8): 533–535.

25. Tzonelih, H., Narn-Yoh, L., Chuang-Ming, L., Ming- Yung, K. and Yung-Hsiang, C. 1995. "Two attacks on Neumann-Stubblebine authentication protocols", *Information Processing Letters,* **53**: 103–107.

26. Tzonelih, H. and Yung-Hsiang, C. 1995. On the security of splice/as : The uthentication system in wide internet. *Information Processing Letters,* **53**: 97-101.

27. Clark, J. and Jacob, J. 1995. On the security of recent protocols. *Information Processing Letters,* **56**(3): 151-155.