Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023

SECURE ZRP PROTOCOL UNDER WORMHOLE ATTACK: A SURVEY REPORT

Mr. Abhinav Kumar, Assistant Professor, Department of Computer Science and Information Technology, ITM College, Dehradun, Uttarakhand

Abstract
The security is an important issue of mobile ad hoc network (MANET) due to every node independently visits in network. When nodes are arranged without topology then chances of attack is more than in networking. In MANET, nodes are organized in without topology due to the nature of network is infrastructure less based network. The different protocols with different natures in MANET when focus on categories of MANET protocols. The three categories of MANET protocol as on demand, table driven and hybrid protocol. In this research paper, focus on hybrid nature protocol. The zone routing protocol (ZRP) is an example of hybrid protocol. The routing attack is divided into two categories as active attack and passive attack. In this paper, use active attack for MANET survey. The wormhole attack is an example of active attack. The security mechanism is divided into four parameters as authentication, authorization, integrity and confidentiality. These Parameters are used in MANET for security under wormhole attack. The objective of this survey paper is review of ZRP protocol in MANET with wormhole attack and security.
Keyword: MANET, ZRP, Routing attack, Wormhole attack, Security, AES

I. Introduction

Wireless network and wired network is two types of communication based network [9]. Wireless network is divided into two parts as infrastructure based and infrastructure less based networks [10]. In infrastructure network, routing nodes are connected with suitable topology and in infrastructure less based network routing nodes are connected without any topology [8]. Mobile ad hoc network is an example of infrastructure less network. Mobile ad hoc network (MANET) is an infrastructure less based network which work on the principle of decentralization and node independency [11]. The biggest limitation of MANET is security of data. The protocols of MANET are divided into three category as reactive, proactive and hybrid protocols [7]. Reactive routing protocol is an on demand based routing protocol which based on the function of routing information and routing discovery example DSR, AODV etc. A proactive routing protocol is based on table driven means every nodes contain routing information in routing table for example OLSR, DSDV etc [3]. A hybrid protocol is a combination of on-demand and table driven routing protocol for example ZRP, LANMARK etc [4]. When a malicious node present in a network then the system is known routing attack in network [12]. The two types of routing attack are active attack and passive attack. In active attack, attacker nodes read and write information in network and in passive attack; attacker node only read information but not change information [8]. A wormhole attack is an example of active attack. A security is a mechanism based on cryptography for protection to data on network. Public (asymmetric) key and private (symmetric) key cryptography are two types of cryptography [1]. AES is an example of symmetric or private key cryptography. In this research survey, proposed the hybrid category of protocol as ZRP, active attack of routing attack as wormhole and symmetric category of security as AES-128 bit [2]. In this research survey the ZRP protocol under wormhole attack with AES security. Following figure 1 show the structure MANET and wormhole attack with security.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023

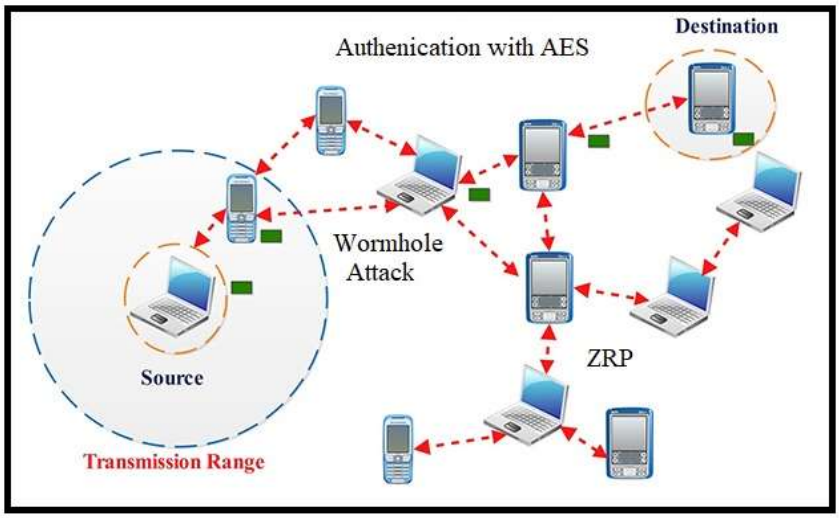

Figure1.Structure of MANET in wormhole attack with security

II. Study of Background

In this section, discuss the basic study of protocol, attacks and security which based on this research review as:

A. ZRP (Zone Routing Protocol): Zone Routing Protocol (ZRP) is a hybrid based (combination to on-demand and table driven) routing protocol that implement on together reactive and proactive routing protocols when send the information on the network [4]. The designer of ZRP for the purpose of reduced overhead processing with data delivery in speed up through select the most capable protocol to apply throughout for the route. Following figure 2 show the nodes structure of ZRP protocol.

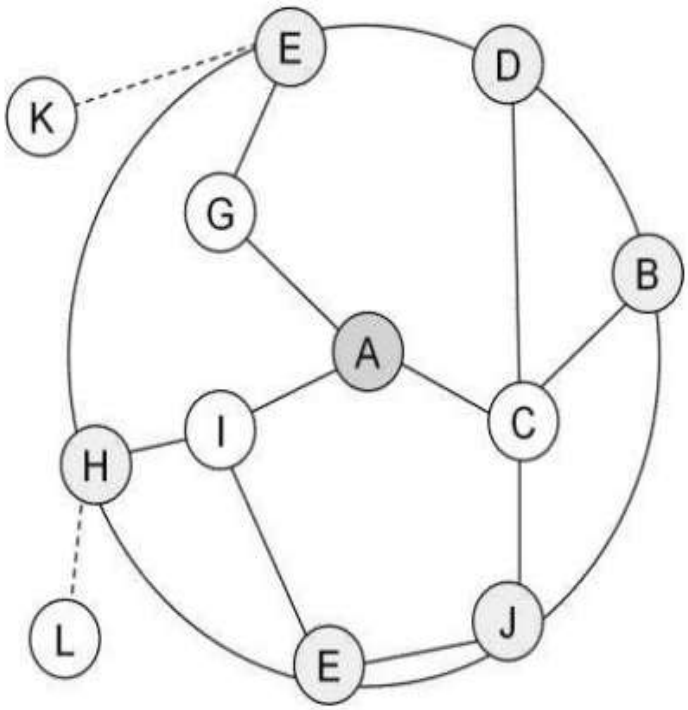

Figure 2.Zone state routing protocol (ZRP)

B. Wormhole Attack: A **wormhole attack is an active attack**. In this attack, an attacker node attacks on data packets (or bits) from one position in the network to other position with retransmit in the network [5]. Figure 3 show the wormhole attack in MANET.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, No. 2, July : 2023

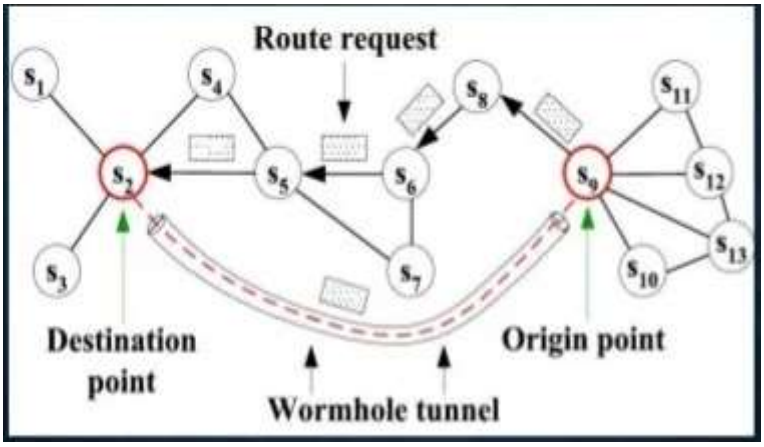

Figure3.structure of wormhole attack in MANET

C. AES (Advanced Encryption Standard): AES execute operations of data on bytes relatively than in bits. The size of cipher text or secure key in AES is 128 bits [6]. This technique is a symmetric based cryptography. Following figure 4 shows the structure of AES in MANET.

Figure 4.Structure of AES in MANET

III. Literature Review

In this section, discuss the review of literature regarding next research work, show in table 1 as:

Author's	Research Category	Research Contribution	Journal's
Hanif, M. et al., (2022)	Wormhole detection by AI in WSN	Proposed the survey of wormhole attack detection using different schemes like AI based, ML based, path selection based mobile agent based schemes [1].	MDPI
Teli, T. A. et al., (2022)	Routing protocols of MANET with attacks and mitigation techniques	Proposed the survey on routing protocol (reactive, proactive and hybrid), routing attacks (blackhole, wormhole and grey-hole) and mitigation techniques. [2]	IJME (Kalahari Journals)

Shankar, T. N., (2022).	Authentic data transmission in ZRP protocol	Proposed the approach for secure data transmission in ZRP protocol for provide to QoS under grey-hole attack [3].	Journal of Scientific & Industrial Research (JSIR)
Jghef, Y. S. et al., (2022)	Secure internet of drone things (SIoDT) based on bio inspired dynamic trust	Proposed the new approach for congestion control and trust estimation as bio inspired dynamic trusted congestion aware zone based internet of drone things (BDTC-SIOVTs) [4].	MDPI
Ajjaj S. et al., (2022)	Statistical design of VANET	Proposed the performance evaluation of VANET protocol under reliability of statistical model using design of experiment methodology with including placket-burman method, full factorial method and taguchi method [5].	MDPI (applied system innovation)
Kaur, G., & Midha, K. (2022)	Security of MANET	Proposed the review of security techniques in MANET protocol under routing attack detection [6].	Mathematical Statistician and Engineering Applications
Tsao, K. Y. et al., (2022)	Solution for UAV communication and FANET (flying ad hoc network) under cyber security threats	Proposed the survey of security for FANET (flying adhoc network) under different threats of cyber attack with solution of cyber security [7].	Ad hoc Networks (Elsevier)
Hussain, S. et al., (2022)	AI based Ant-routing protocol in flying network for secure communication	Proposed the ant colony optimization based routing protocol for secure and optimal communication in AI based flying networks for searching and rescue operation with proper monitoring [8].	Hindawi (Applied Computational Intelligence and Soft Computing)

Govindasamy, J., & Punniakody, S. (2018)	Performance comparison between MANET protocol under wormhole attack in WSN	Proposed the performance investigation of reactive routing (AODV), proactive routing (OLSR) and hybrid routing (ZRP) protocol under wormhole attack in WSN [9].	Science Direct (Elsevier)

Table1.Literature Review

IV. Research Gaps

In this section, discuss the research gaps which observed by literature survey for make research objectives as:

A. The detection and avoidance of wormhole attack is a gap of research [1].

B. Effect of detection on performance matrices as packet delivery ratio (PDR), routing overhead and, end to end delay (EED) in same time under attacks [2].

C. In this research, only access based enumeration (ABE) is used for security in ZRP under QoS factors [3].

D. Performance is low when falsifications attack on position [4].

E. Security issues in traditional routing protocol under detection of routing attack [6].

F. Restricted computational ability, highly mobile nodes, topology change frequently in FANET [7].

G. Require the design of ZRP in terms of secure routing protocol for prevent the security threats [9].

V. Research Challenges

In this section, focus on challenges of research which conducted from research gaps on behalf of literature survey. The research objective of this work as:

A. Performance analysis of ZRP protocol in different time under wormhole attack detection.

B. Security of ZRP protocol using AES-128 bit security under wormhole detection.

C. Performance evaluation between ZRP and traditional protocol under attack detection.

D. Security solution in low power computation in MANET.

E. Security design of ZRP protocol under attack detection.

VI. Conclusion and Future Scope

Mobile ad hoc network (MANET) is decentralized based infrastructure less network. The security is mostly drawbacks in MANET due to nodes are independently visited in network. In this review paper, propose the conceptual study of MANET under wormhole attack with security. This completely study is based on previous research papers and presents the research gaps of theses research papers. The future scope of this research article is implementation of different challenges generated by research gaps and the practical implementation of this survey paper with proper simulation tool in different parameters.

References

[1] Hanif, M., Ashraf, H., Jalil, Z., Jhanjhi, N. Z., Humayun, M., Saeed, S., & Almuhaideb, A. M. (2022). AI-Based Wormhole Attack Detection Techniques in Wireless Sensor Networks. Electronics, 11(15), 2324.

[2] Teli, T. A., Yousuf, R., & Khan, D. A. (2022). MANET Routing Protocols Attacks and Mitigation Techniques: A Review. International Journal of Mechanical Engineering, 7(2), 1468-1478.

[3] Shankar, T. N. (2022). Hybrid Energy Efficient Secured Attribute based ZRP Aiding Authentic Data Transmission. Journal of Scientific & Industrial Research, 81(01), 69-75.

[4] Jghef, Y. S., Jasim, M. J. M., Ghanimi, H. M., Algarni, A. D., Soliman, N. F., El-Shafai, W., ... & Abbas, F. H. (2022). Bio-Inspired Dynamic Trust and Congestion-Aware Zone-Based Secured Internet of Drone Things (SIoDT). Drones, 6(11), 337.

[5] Ajjaj, S., El Houssaini, S., Hain, M., & El Houssaini, M. A. (2022). Performance assessment and modeling of routing protocol in vehicular ad hoc networks using statistical design of experiments methodology: A comprehensive study. Applied System Innovation, 5(1), 19.

[6] Kaur, G., & Midha, K. (2022). Review of MANET Security Features. Mathematical Statistician and Engineering Applications, 71(4), 2430-2439.

[7] Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. Ad Hoc Networks, 133, 102894.

[8] Hussain, S., Ahmed, S., Thasin, A., & Saad, R. M. (2022). AI-Enabled Ant-Routing Protocol to Secure Communication in Flying Networks. Applied Computational Intelligence and Soft Computing, 2022.

[9] 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.

[10] Chaubey, N., Aggarwal, A., Gandhi, S., & Jani, K. A. (2015, February). Performance analysis of TSDRP and AODV routing protocol under black hole attacks in manets by varying network size. In 2015 Fifth International Conference on Advanced Computing & Communication Technologies (pp. 320-324). IEEE.

[11] Kumar, J., Kulkarni, M., & Gupta, D. (2013). Effect of Black hole Attack on MANET routing protocols. International Journal of Computer Network and Information Security, 5(5), 64.

[12] Raj, P. N., & Swadas, P. B. (2009). Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. arXiv preprint arXiv:0909.2371.