Deo Prakash et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 4, Issue 1o, Month 2017, pp.170-174

A Survey on Security Attacks and Countermeasures in Mobile AdHoc Networks for Secure Data Dissemination

Deo Prakash[1,*], Neeraj Kumar[2], M.L. Garg[3]

School of Computer Science & Engineering, Faculty of Engineering, SMVD University, Katra, India
Department of Computer Science & Engineering, Thapar University, Patiala, India
Department of Computer Science and Engineering, DIT University, Dehradun, India

*E-Mail: deoprakash.a@gmail.com

Abstract-**Security has been significant issue in computer networks. It becomes more critical issue when we come to the wireless networks and specifically Mobile AdHoc Networks (MANETs). There have been a number of security attacks in Mobile AdHoc networks but Black Hole and Gray Hole attacks are most popular attacks among all. This paper presents a survey on Black Hole and Gray Hole attacks and countermeasures for Secure Data Dissemination.**

Keywords—MANET, Security Attacks, Black Hole Attack, Gray Hole Attack, Secure Data Dissemination.

I. Introduction

Since the inception of computer networks security remains very critical issue.
In wireless network, the route is dynamically selected on the basis of various network parameters and the corresponding routing entries are calculated at each hop to maintain the record of the route. New entries are calculated if the old one(s) are affected by factors such as change in topology.
[1] Presents well known Diffie-Hellman algorithm for key exchange which is used in most of the key exchange cases till date. [2] Presents the MD5 Message-Digest Algorithm for securing data. Since there is no fixed position in MANETs, the Global positioning type of route selection mechanism becomes very important. AODV [3] is key protocol of MANETs which actually is prone to the security attacks.
Over the few years some security protocols have been proposed by research community for MANETs. These protocols are studied form different perspective keeping in view of the properties and constraints of these networks. There are a number of types of attacks however the main security attacks in Mobile Ad Hoc Networks are the Black Hole and Gray Hole attacks. Here a systematic literature review is given over the period.

II. Review on Various Security Attacks and Countermeasures

Tamilselvan et. al.[4] focused on the importance of AODV (Ad hoc on demand Distance Vector) protocol and its security issues. Security issues particularly the black hole attack is discussed in the paper. They discussed about detecting the malicious node in the network and then removing that node from the network.

Djenouri et. al.[5] Proposed a novel monitoring approach to tackle the denial of service attack which uses the Bayesian technique for the purpose of judgment.
Mary et. al.[6] presents mobile ad hoc networks with nodes having their own mobility and connected with each other using the wireless links for communication. They also describes about the dynamic nature of the ad hoc network and hence discusses the different vulnerabilities in the networks. Paper discusses the techniques on how to achieve the security measures in the process of communication. While the discussion of security black hole attack was discussed and along with it malicious nodes and their effects are also discussed. This technique uses advertising to find the shortest path from the source node to the destination node. The proposed scheme in the paper aims on using Multicast Ad-hoc On Demand Distance Vector Routing (MAODV) for the implementation purpose.
Subathra et. al.[7] describes the mobile ad hoc network as the collection of wireless nodes responsible for communication without the help of infrastructure. As it is infrastructure less and hence nodes play a key role in providing the functionality of the infrastructure as much as possible. The author also points out the importance of Dynamic Source Routing (DSR) in the mobile ad hoc network but on the other hand also points out the security issues with the corresponding protocol. The most significant attack on the network being the black hole attack with the help of malicious nodes. The author proposes a solution to discover a secure route from the source to the destination by avoiding the malicious nodes.
Bhalaji et. al.[8] aims to focus on the problems encountered by the ad hoc networks. The author's research was based on a cooperative environment. The primary aim of this paper was to focus on the security and multi hop problem faced by the mobile ad hoc networks. It was observed that security problems were comparatively more in wireless communication when compared to wired ones. They also

discusses about the black hole attack along with the cooperative black hole attack.

Tseng et. al.[9] Presented the black hole attack that prevail in the mobile ad hoc networks with the nodes having their own mobility. The security issues have been discussed in this paper related to the black hole attack. In this paper a survey has been done on the existing solution to these attacks and found out merits and demerits related to these techniques.

Umaparvathi et. al.[10] discusses about the mobile ad hoc network for the purpose of communication between the two different nodes. An important concept to keep in mind is that the packets that are sent from the source to the destination contain a number of intermediate nodes. Bringing the security reasons into consideration as it is easy to intercept the message as the message is supposed to flow through the node and modifying the node is also easy and a major security breech. One of such attack is the black hole attack that has been discussed in the paper by the author.

Sen[11] discussed about mobile ad hoc network which is described as collection of nodes for the purpose of communication using the multi hop technique. The author of this paper tries to give his opinion on the security concerns and its preventions. Out of all the layers in the OSI model the main reason of concern is the network layer and in this paper the challenges related to the network layer are discussed. To achieve all the goals Ad hoc on demand distance vector routing (AODV) is used. The most popular attack (Black hole attack) and its consequences are discussed with simulations. The only disadvantage being that the proposed mechanism is not applicable on the cryptographic system.

Su[12] describes the black hole attack on the mobile ad hoc network which is performed with the help of malicious nodes as forcefully acquiring the complete route from the source to the destination. A specific type of attack being the selective black hole attack in which malicious node selectively drops the packets coming from the source and tries to act as a normal node. This paper focuses its attention on the intrusion detection system on the mobile ad hoc network for the purpose of detection and then prevention from the selective black hole attack. Focus is given on the sniff mode while transmission takes place. Works with the concept of suspicion value and the concept of thresholding. Once the threshold value is exceeded the broadcasting of block message is send to all the nodes.

Mohanapriya et. al.[13] presented the performance in the DSR protocol and provide a solution for the attack called Enhanced Dynamic Source Routing (EDSR) Protocol. It detects the no packets reaching the destination and detects the blackhole. The protocol results in increase in packet delivery and loss in packet loss ratio.

Yi at. al. [14] Described an adaptive approach to detect the blackhole using the path based method on the next hop action .It uses a collision detection method to detect the malicious nodes which helps in saving the resources. The method used with DSR helped to improve detection rate as it becomes more than 90%.

Umaparvathi et. al.[15] Considers a fact that the communication process between the nodes needs cooperation from other nodes. The information interception and modification is considered in this paper. This paper also discusses the impact of black hole attack on the communication network. The proposed mechanism is a secure routing protocol named as Two Tier secure Adhoc On-Demand Distance Vector (TTSAODV) which is a modification to Adhoc On-Demand Distance Vector (AODV) routing protocol.

Usha[16] in this paper is trying to say that the most prone attack in the MANETS are the blackhole attack because of the dynamic infrastructure and the freely moving mobile nodes.Mostly in blackhole attacks the packets are dropped and the routes are changed.The simulation uses the AODV protocol and the results showed that that the packet drop drastically and the overhead as well as packet delivery ratio increases leading to the deterioration of the MANET.

Medadianet.al.[17] discussed about the black hole attack that prevails in the mobile ad hoc networks. This paper considers a network with mobile nodes and wireless links for the purpose of communication. The main protocol that is used for the implementation is Ad hoc networks is AODV (Ad hoc on demand Distance Vector) protocol. Keeping the security issues in mind the author also focuses on the black hole attack that is prevalent in the mobile ad hoc network. The author also kept malicious nodes in mind while simulation is carried out.

Arunmozhi et. al.[18] talks about the mobile ad hoc network with mobile nodes having their own speed. An attack on mobile ad hoc network i.e. black hole attack is discussed with its security concerns. It is observed by various authors that the network traffic can be obtained from the network which is also considered as an attack. The author takes a defensive scheme for the purpose of detecting a black hole node in the paper. As the author keeps the security measures in mind, the use of destination sequence number is used which are updated dynamically.

Mahmood et. al. [19] Presented a black hole attack which consists of both the random as well as the critical nodes. in both critical nodes are important as they are present in most of the paths from source to the destination. The new attack affects the packet delivery ratio, overhead and delay drastically.

Peer et. al. [20] Presented both the attacks i.e. wormhole and blackhole attacks in secure VBOR for MANETs. VBOR is the base and the keys are exchanged with the help of the residual energy of the nodes.

Zougagh et. al.[21] Reported an attack in which the nodes which are adjacent to each other cooperate and helps in finding the intrusion, prevent the disruption of the topology and keep a check on the no of route to the destination node.

Mohanapriya et. al.[22] Analysed the performance in the DSR protocol and provide a solution for the attack called Enhanced Dynamic Source Routing (EDSR) Protocol. It detects the no packets reaching the destination and detects the blackhole. The protocol results in increase in packet delivery and loss in packet loss ratio.

Baadache et. al.[23] Proposed an end to end acknowledgement method for black hole attack in MANETs. They included acknowledgement of the message at the senders and at the destination. If any anomaly is found between it checks the route through which the packets were forward. The detection ratio, delivery ratio and additional

overhead improve as compare to the previous 2 hop ACK and watchdog approach.

Rajesh et. al.[24]evaluated the performance of DSR protocol under the black hole attack scenario. They showed that the throughput degrades by significantly as well as the end to end delay increases drastically when simulated with Dynamic Source Routing Protocol.

Mohanapriya et. al.[25] Proposed a Modified Dynamic Source routing Protocol (MDSR) which includes the Intrusion Detection System (IDS) mainly designed for the selective blackhole attack in which the packets are dropped selectively.The IDS detects the indifferent behaviour and the block message is passed to all the nodes to isolate the blackhole.

Selvavinayaki et. al.[26] Proposed a New Enhanced Proactive Secret Sharing Scheme (NEPSSS) to maintain the data confidentiality, integrity and authenticity. The proposed algorithm consists of mainly two parts one is to achieve trust and second is to provide data authenticity and integrity. The simulation points to the better packet delivery ratio, decrease in delays and less packet overhead.

Ahmed et. al.[27] proposed approach used a reliable and low control overhead approach named as the bullet proof verification method consisting of two phase detection and verification. In detection a suspicious node is found and in verification an encrypted verification message is passed through the whole route to check the suspicion in the hop count, destination sequence number or the hop distance. They claimed better simulation results decreasing the probability of a black hole attack.

Baburaj et. al.[28] proposed an efficient routing mechanism for prevention of both the key attacks i.e. wormhole as well as black-hole attacks. DTN or Distribution Tolerant Networks are wireless communication methods with no path between the source and the destination that is why they are prone to the common blac-khole and wormhole attack which are certainly caused by change in the RREP's. These attacks are responsible for the transfer of packets to the suspicious location. The lack of proper security is the reason for non identification of proper valid routes. To counter with this problem a novel key generation mechanism is introduced which consequently provide security to the wireless network. They have supported their mechanism with the help of simulations.

Zougagh et. al.[29] reported a novel approach in OLSR for detecting black hole attack. The nodes uses protocol like Optimised link state protocol to communicate with each other. They proposes a cooperative black hole attack in which the nodes coordinate with each other to analyze the neighborhood .This prevents routes to the target node.

Ding et. al.[30] reported a black hole attack model and simulated it for showing that the main malicious activities take place on AODV. It is fact that due to wide application of the MANETS the security has become an important issue to counter the black hole attacks .The blackhole attacks vulnerabilities are found mainly by using it with AODV protocol on the NS2 network by taking different malicious nodes and simulating it at different intensities. The different results pave way for the researchers to research on the new security advancements in the fields of the MANET security.

Hu et. al. [31] presented the attacks against routing in ad hoc networks, and the design and performance evaluation of a new secure on-demand ad hoc network routing protocol which they gave the name Ariadne. They also disabused about attackers from tampering with uncompromised routes which consists of uncompromised nodes, and also from a number of Denial-of-Service attacks. They presented the general idea of various attacks and the various preventive approaches to prevent the attacks. Imrich Chlamtac et. al. [32] describes a survey on the then challenges in MANETs.

Papadimitratos et al. [33, 34] reported SMT, Hu et al. [35] proposed SEAD, Wu et al. [36] presented a survey, Li et al. [37] proposed a routing security algorithm, Komninos et al. [38] reported the main security issues in MANETs. Xiaopeng et al. [39] talks about Grayhole attack, Mavropodi [40] proposed SecMR, Komninos et al. [41] presented the layered security mechanism, Zhao et al. [42], Marchang et al. [43] and Yeun et al. [44] also proposed the security approaches related to the same area. Cordasco et al. [45] compared SAODV and TAODV. Kim et al [46], Dutta et al. [47], Su [48] proposed WARP, Makri et al. [49] and Su [50] also taken care about the security concern of MANETs. Khalil et al. [51] and Mulert et al. [52] presented the security issue in their own way including the simulation to the case study type reports. Bhalaji et al. [53] reported Grayhole attack with Dynamic nature.

III. Conclusion

In this paper we reviewed a number of papers related to security attacks in Mobile AdHoc Networks. We reviewed the Black Hole Attacks and Also the Gray Hole Attacks and their countermeasures for secure data dissemination.

REFERENCES

[1]W. Diffie, M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, Volume 22, Issue 6, 1976

[2]R. Rivest, The MD5 Message-Digest Algorithm, 1991 (https://tools.ietf.org/html/rfc1321)

[3]C. Perkins, E. Royer, Ad hoc On-demand Distance Vector Routing, in: Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications, 1999, pp. 99–100.

[4]Tamilselvan L., Sankaranarayanan V., Prevention of co-operative black hole attack in MANET, Journal of Networks, Volume 3, Issue 5, Pages 13-20, 2008

[5]Djenouri D., Badache N., Struggling against selfishness and black hole attacks in MANETs, Wireless Communications and Mobile Computing, Volume 8, Issue 6, Pages 689-704, 2008

[6]Mary Anita E.A., Vasudevan V., Prevention of black hole attack in multicast routing protocols for mobile ad-hoc networks using a self-organized public key infrastructure, Information Security Journal, Volume 18, Issue 5, Pages 248-256, 2009

[7]Subathra P., Sivagurunathan S., Ramaraj N., Detection and prevention of single and cooperative black hole attacks in mobile ad hoc networks, International Journal of Business Data Communications and Networking, Volume 6, Issue 1, Pages 40-59, 2010

[8]Bhalaji N., Shanmugam A., A trust based model to mitigate black hole attacks in DSR based MANETs, European Journal of Scientific Research, Volume 50, Issue 1, Pages 6-15, 2011
[9]Tseng F.-H., Chou L.-D., Chao H.-C., A survey of black hole attacks in wireless mobile ad hoc networks, Human-centric Computing and Information Sciences, Volume 1, Issue 1, Pages 1- 16, 2011
[10]Umaparvathi M., Varughese D.K., Secure video transmission against black hole attack in MANETs, International Journal of Business Data Communications and Networking, Volume 7, Issue 4, Pages 1-17, 2011
[11]Sen J., Detection of cooperative black hole attack in wireless ad hoc networks, International Journal of Simulation: Systems, Science and Technology, Volume 12, Issue 4, Pages 25-33, 2011
[12]Su M.-Y., Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems, Computer Communications, Volume 34, Issue 1, Pages 107-117, 2011
[13]Mohanapriya M., Krishnamurthi I., Enhanced dynamic source routing protocol for mitigating black hole attack, International Journal of Wireless and Mobile Computing, Volume 5, Issue 4, Pages 341- 350, 2012
[14]Yi P., Zhu T., Liu N., Wu Y., Li J., Cross-layer detection for black hole attack in wireless network, Journal of Computational Information Systems, Volume 8, Issue 10, Pages 4101-4109, 2012
[15]Umaparvathi M., Varughese D.K., Two Tier secure AODV against black hole attack in MANETs, European Journal of Scientific Research, Volume 72, Issue 3, Pages 369-382, 2012
[16]Usha Bose, Understanding black hole attack in MANETs, European Journal of Scientific Research, Volume 83, Issue 3, Pages 383- 396, 2012
[17]Medadian M., Fardad K., Proposing a method to detect black hole attacks in AODV routing protocol, European Journal of Scientific Research, Volume 69, Issue 1, Pages 100-110, 2012
[18]Arunmozhi S.A., Venkataramani Y., Black Hole Attack Detection and Performance Improvement in Mobile Ad-Hoc Network, Information Security Journal, Volume 21, Issue 3, Pages 150-158, 2012
[19]Mahmood R.A.R., Hanapi Z.M., Hasan S., Khan A., Effective black hole attacks in MANETs, Journal of Computer Science, Volume 9, Issue 12, Pages 1722- 1733, 2013
[20]Peer Meera Labbai T., Rajamani V., Prevention of worm hole and black hole attacks in secure VBOR for mobile ad hoc networks, Journal of Theoretical and Applied Information Technology, Volume 55, Issue 2, Pages 190-196, 2013
[21]Zougagh H., Toumanari A., Latif R., Idboufker N., A new solution to defend against cooperative black hole attack in optimized link state routing protocol, International Review on Computers and Software, Volume 8, Issue 2, Pages 519-526, 2013
[22]Mohanapriya M., Krishnamurthi I., A light-weight and scalable solution for secure routing in DSR MANET for black hole attack, Ad-Hoc and Sensor Wireless Networks, Volume 17, Issue 2-Jan, Pages 33-52, 2013
[23]Baadache A., Belmehdi A., Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks, Computer Networks, Volume 73, Pages 173-184, 2014
[24]Rajesh kumar G., Valluvan K.R., Performance evaluation of dynamic source routing under black hole attack, Journal of Theoretical and Applied Information Technology, Volume 66, Issue 1, Pages 290-297, 2014
[25]Mohanapriya M., Krishnamurthi I., Modified DSR protocol for detection and removal of selective black hole attack in MANET, Computers and Electrical Engineering, Volume 40, Issue 2, Pages 530-538, 2014
[26]Selvavinayaki K., Karthikeyan E., A secured data transmission method using enhanced proactive secret sharing scheme to prevent black hole attacks in MANETs, Journal of Theoretical and Applied Information Technology, Volume 67, Issue 3, Pages 554-561, 2014
[27]Ahmed F., Yoon S., Oh H., A bullet-proof verification approach to defend against black hole attacks in mobile ad hoc networks, IEICE Transactions on Communications, Volume E98B, Issue 3, Pages 422-436, 2015
[28]Baburaj C.A., Alagarsamy K., An efficient secure routing mechanism for preventing wormhole and black hole attacks in a trusted DTN environment, International Journal of Wireless and Mobile Computing, Volume 9, Issue 2, Pages 140-147, 2015
[29]Zougagh H., Toumanari A., Latif R., Idboufker N., A novel security approach for struggling black hole attack in optimised link state routing protocol, International Journal of Sensor Networks, Volume 18, Issue 2-Jan, Pages 101-110, 2015
[30]Ding Y., Qu H., Li G., Black hole attack model and simulation for mobile Ad Hoc network, International Journal of Innovative Computing, Information and Control, Volume 11, Issue 1, Pages 203-211, 2015
[31]Yih-Chun Hu, Adrian Perrig, David B. Johnson, Ariadne: A Secure On-Demand Routing Protocol for AdHoc Networks, MobiCom'02, September 23–26, 2002, Atlanta, Georgia, USA.
[32]Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, Mobile ad hoc networking: imperatives and challenges, Ad Hoc Networks 1 (2003) 13–64
[33]Panagiotis Papadimitratos, Zygmunt J. Haas, Secure Data Transmission in Mobile Ad Hoc Networks, ACM Workshop on Wireless Security (WiSe 2003), San Diego, CA, September 19, 2003
[34]Panagiotis Papadimitratos , Zygmunt J. Haas, Secure message transmission in mobile ad hoc networks, Ad Hoc Networks, 1: 1, 193–209, 2003
[35]Yih-Chun Hu, David B. Johnson, Adrian Perrig, SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks, Ad Hoc Networks, 1: 1, 175–192, 2003
[36]Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, WIRELESS/MOBILE NETWORK SECURITY, Chapter 12, 1-38, 2006
[37]Jung-Shian Li, Cheng-Ta Lee, Improve routing trust with promiscuous listening routing security algorithm in mobile ad hoc networks, Computer Communications 29 (2006) 1121–1132

[38]Nikos Komninos, Dimitris Vergados, Christos Douligeris, Layered security design for mobile ad hoc networks, computers & security 25(2006)121–130
[39]Gao Xiaopeng, A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks, IFIP International Conference on Network and Parallel Computing Workshops, Page(s): 209 – 214, BeiHang Univ., Beijing, Date of Conference: 18-21 Sept. 2007
[40]Rosa Mavropodi, Panayiotis Kotzanikolaou, Christos Douligeris, SecMR – a secure multipath routing protocol for ad hoc networks, Ad Hoc Networks 5 (2007) 87–99
[41]Nikos Komninos, Dimitrios D. Vergados, Christos Douligeris, Authentication in a layered security approach for mobile ad hoc networks, computers &security 26(2007)373–380
[42]Shushan Zhao, Akshai Aggarwal, Shuping Liu, Huapeng Wu, A Secure Routing Protocol in Proactive Security Approach for Mobile Ad-hoc Networks, IEEE Wireless Communications and Networking Conference(WCNC), pp. 2627 – 2632, Univ. of Windsor, Windsor, March 31, 2008-April 3, 2008
[43]Ningrinla Marchang, Raja Datta, Collaborative techniques for intrusion detection in mobile ad-hoc networks, Ad Hoc Networks 6 (2008) 508–523
[44]Chan Yeob Yeun, Kyusuk Han, Duc Liem Vo, Kwangjo Kim, Secure authenticated group key agreement protocol in the MANET environment, Information Security Technical Report 13(2008)158–164
[45]Jared Cordasco, Susanne Wetzel, Cryptographic Versus Trust-based Methods for MANET Routing Security, Electronic Notes in Theoretical Computer Science 197 (2008) 131–140
[46]Jihye Kim, Gene Tsudik, SRDP: Secure route discovery for dynamic source routing in MANETs, Ad Hoc Networks 7 (2009) 1097–1109
[47]Ratna Dutta, Sourav Mukhopadhyay, Martin Collier, Computationally secure self-healing key distribution with revocation in wireless ad hoc networks, Ad Hoc Networks, 8: 6, 597-613, 2010.
[48]Ming-Yang Su, WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks, computers & Security 29(2010)208–224
[49]Eleftheria Makri, Elisavet Konstantinou, Constant round group key agreement protocols: A comparative study, computers & Security 30(2011)643–678
[50]Ming-Yang Su, Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems, Computer Communications 34 (2011) 107–117
[51]Issa Khalil, Mamoun Awad, Abdallah Khreishah, CTAC: Control traffic tunneling attacks' countermeasures in mobile wireless networks, Computer Networks 56 (2012) 3300–3317
[52]Jan von Mulert, IanWelch, Winston K. G. Seah, Security threats and solutions in MANETs: A case study using AODV and SAODV, Journal of Network and Computer Applications 35 (2012) 1249–1259
[53]N. Bhalaji, A.Shanmugam, Dynamic Trust Based Method to Mitigate Greyhole Attack in Mobile Adhoc Networks, Procedia Engineering 30 (2012) 881 – 888

