INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

DETECTION OF BLACK HOLE ATTACK IN MOBILE AD HOC NETWORKS: A SURVEY

Harmanpreet Kaur[1], P. S. Mann[2]

Research Scholar in Computer Science and Engineering Department[1], harmanpreet.3005@gmail.com[1]

Faculty of IT Department[2], psmaan@hotmail.com[2]

Author Correspondence: DAV Institute of Engineering and Technology [1, 2], Jalandhar (Punjab), India,

9876700386 [1], 9888395367[2], harmanpreet.3005@gmail.com[1], psmaan@hotmail.com[2]

Abstract

The rapid growth in the field of mobile computing is forcing an alternative method for mobile communication, in which mobile devices form a self-created, self-organized and self-administered wireless networks that are known as mobile ad hoc network. Due to MANETs don't require the infrastructure, it can install fast and suitably in any environment. Because of its simple deployment features, MANETs can be used in personal area networks, home area networks etc. Specially, MANETs go with for military operations and the developing disasters rescue that need to conquer topography and special purpose in urgent. However, due to their inbuilt characteristics of dynamic topology and lack of centralized access point security, MANET is open to various kinds of attacks. The success of mobile ad hoc networks (MANET) robustly depends on people's confidence towards its security. MANET security is a complex and challenging topic and it is a vital service for wired and wireless network communications. In this paper various security attacks that are possible in the network are discussed and Defensive Mechanisms against a well-known attack (i.e. Black hole attack) are put forward.

Keywords: MANETs, Security Requirements, Security Attacks, Security measures against Black hole Attack.

1. Introduction

MANET [1] is a collection of mobile nodes which does not need any central access point or base station. They exploit wireless connections to attach to various networks like standard Wi-Fi connection, or another medium, like cellular or satellite transmission. Some of the MANETs are limited to a local area of wireless devices (such as a collection of laptop computers), while others may be linked to the Internet. Because of the dynamic life of MANETs, they are normally not very secure, so it is important to be careful what data is sent over a MANET. Various types of attacks are possible in the network that carries data among various nodes.

So in short, it can be concluded that ad hoc networks:

- Do not need backbone infrastructure,
- Are easy to deploy,
- Valuable when infrastructure is absent, destroyed or impractical.

The set of applications for MANETs [2] is varied, ranging from small, static networks that are controlled by power sources, to large-scale, mobile, highly lively networks. For example: Personal area networking(cell phone, laptop, ear phone, wrist watch), Civilian environments(taxi cab network, meeting rooms, sports stadiums), Military environments(soldiers, tanks, planes), Emergency operations(policing and fire fighting).

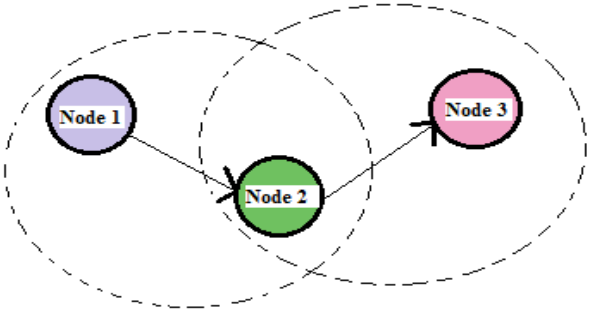

Figure 1: Example of mobile ad-hoc network [3]

1.1 Characteristics of MANET [4]

- In MANET, each node acts as both host and router. That is it is self-directed in behavior.
- MANETs are competent of multi-hop routing.
- A centralized firewall is not present thus it has distributed nature of operation for security, routing and host design.
- The nature of network topology is dynamic.
- Mobile nodes are differentiated from others with less memory, power and light weight features.
- The reliability, efficiency, stability and capacity of wireless links are often lesser when compared with wired links.
- Node connectivity is alternating.
- MANETs form a completely symmetric atmosphere.

1.2 MANET Challenges

A MANET environment has to conquer certain issues of limitation and inadequacy. It includes:

- The wireless link uniqueness is time-unreliable in nature.
- It has limited range of wireless transmission.
- MANETs skill higher packet loss due to errors in broadcast.
- The dynamic nature of network topology outcome in frequent path breaks.
- The random association of nodes often leads to division of the network.

The remainder of this paper is organized as follows: Section 2 reviews Security and various attacks in MANETs. Section 3 describes solutions to Black hole attacks. Finally, the section 4 is conclusion that concludes the main text followed by references that completes the article.

2. Security in MANETs

Security [3] is an important requirement in MANETS. Compared to wired networks, MANETs are more exposed to security attacks due to lack of centralized authority and restricted resources. Attacks on ad hoc networks can be classified as passive and active attacks, depending on whether the usual operation of the network is disrupted or not. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad hoc network environment. They are namely: Confidentiality **(**it makes sure that only authorized sensor node is accessing the content of messages), Availability **(**it ensures that services should be available by WSN whenever it is required), Integrity **(**it measures that received data has not been modified by an adversary**),** Authentication **(**it empowers a node

to guarantee the identity of neighbor to which it is communicating) and Authorization (it guarantees that only legal sensor can provide information to network).

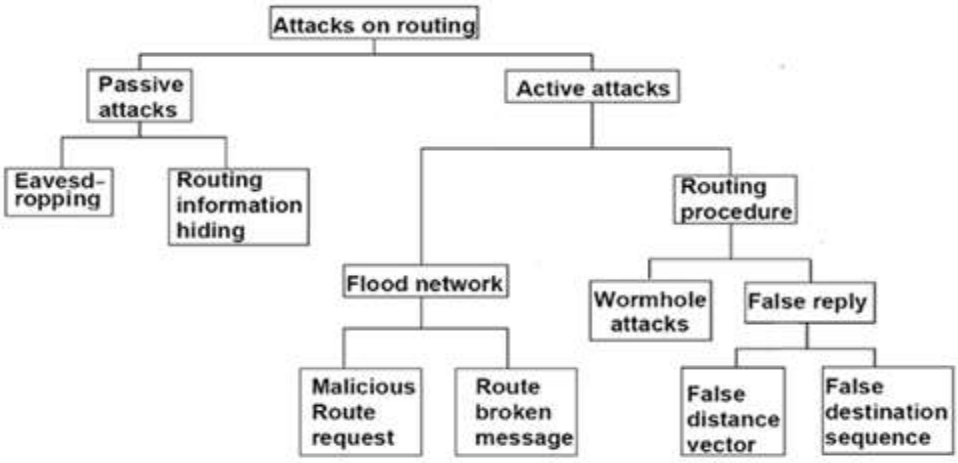

Figure 2: Classification of attack on routing [4]

2.1 Type of Security Attacks

The security attacks in MANET can be generally classified into: passive attacks and active attacks.

Passive Attacks
A passive attack does not disrupt the usual operation of the network; the attacker the data exchanged in the network without altering it. Here the condition of confidentiality gets debased. Detection of passive attack is very complicated since the operation of the network itself doesn't get affected. One of the ways to remove the problem is to use authoritative encryption mechanism to encrypt the data being transmitted, thereby building it impossible for the attacker to get valuable information from the data overhead.

Active Attacks
An active attack attempts to modify or demolish the data being exchanged in the network there by upsetting the normal performance of the network. Active attacks are of two types: internal or external. Nodes that do not fit in to the network cause external attacks and internal attacks are carried out by compromised nodes that are part of the network. Since the invader is previously part of the network, internal attacks are more cruel and hard to notice than external attacks.

2.2 Various attacks in MANETS [6]

Black hole attack: A black hole attacker first wants to invade into the multicast forwarding set (e.g., by implementing rushing attack) in order to interrupt data packets of the multicast assembly. It then drops several or all data packets it receives instead of forwarding them to the next node on the steering path. This type of attack frequently results in very little packet delivery ratio.

Neighbor attack: Upon getting a packet, an intermediary node records its ID in the packet before forwarding the packet to the subsequent node. An attacker merely forwards the packet without recording its ID in the packet to

create two nodes that are not within the communication range of each other believe that they are neighbors (i.e., one-hop away from each other), ensuing in a disrupted route.

Jellyfish attack: A jellyfish attacker first desires to break in into the multicast forwarding group. It then delays data packets unreasonably for a few amount of time before forwarding them. This outcome in significantly high end-to-end delays and thus degrades the performance of real-time applications.

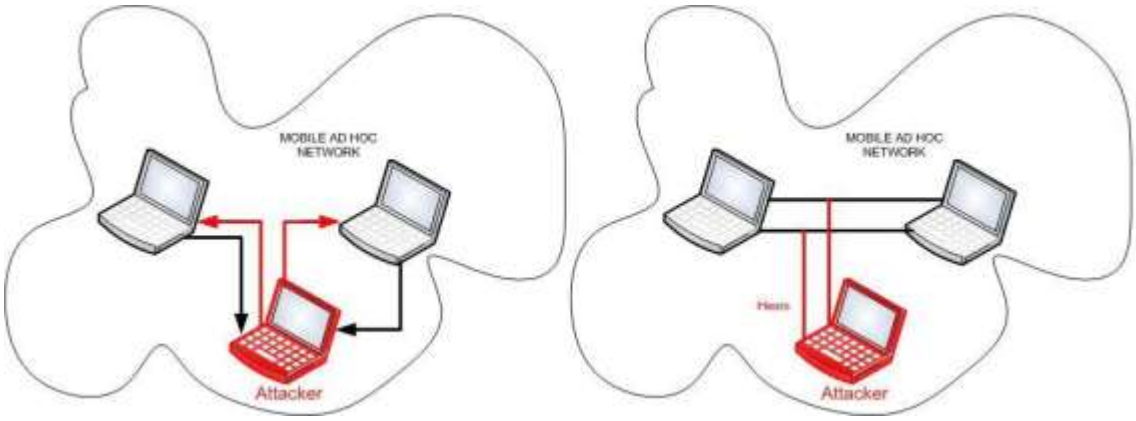

Figure 3: Active and Passive attacks in MANETs [6]

Wormhole attack: An attacker records packets at one position in the network and routes them to a different location. Routing can be troubled when routing control messages are tunneled. This tunnel among two colluding attackers is referred as a wormhole. Wormhole attacks are harsh threats to MANET routing protocols.

3. Solutions to the Black hole Attack

Author Wenjia Li, Anupam Joshi, and Tim Finin [7], a novel idea to order the hubs on the foundation of their practices. They proposed a Support Vector Machine based trust plan. In this plan creator utilized the conduct measurements e.g. Bundle Drop Rate (PDR), Packet Modification Rate (PMR) and Packet Misrouted Rate to start trust around hubs.

Author Bo-Cang Peng, and Chiu-Kuo Liang [8], has proposed the thought of kinship table for enlightening of interruption on MANET. Kinship table is utilized to accumulate the relationship status of all hubs with its neighbors. There are two sections in this table. In first section the identifier of its entire neighboring hub and in second segment, its relationship rank with the neighbor hub that could be companion, acquaintance or outcast. This table is eluded untouched when any hub appropriates the parcels. Firstly hub treats it as more interesting and if the confidence worth is finest hub will treat as copartner, if hub accepts a few bundles from hub effectively, then confidence level is quite high and the hub is acknowledged as a companion.

Author Douglas S. J. De Couto, Daniel Aguayo, John Bicket, and Robert Morris [9], has evaluated a clever thought to discover dark and light black gap hubs, the sender infrequently check through all accessible courses to recognize if the goal appropriated each of its messages clean. With a specific end goal to stay away from any dark gap hubs that may hinder with message movement, the sender telecasts "check" solicitation message and the end of the line's answer might accompany the comparable course as the appeal.

Author D.m. Shila, and T. Anjali [10], has evaluated an answer for monitor particular sending strike (light black opening ambush) in Networks. The principal venture of the calculation is Counter-Threshold Based and it utilizes the edifying edge and parcel counter to arrange ambushes. The following step is Query- Based and it utilizes affirmation from the halfway hubs to confine the ambusher.

Author X.p. Gao, and W. Chen [11], has foreseen to use total mark calculation to guide out bundle declining hubs. The framework comprises of three brought together calculations: Creating evidence calculation; Recognition calculation; Checkup calculation.

Author Hongmei Deng, Wei Li, and Dharma P. Agrawal [12], has proposed the thought of an explanation for single dark gap hub ID. In this each middle hub is utilized to send back the following jump data when it sends back a RREP message. In the wake of accepting the answer message, the source hub don't send the information parcels however extricate the following jump data from the answer bundle and a while later it sends a Further-Request to its next bounce to affirm that it has a path to the middle hub which sends back the Further answer message, and that it has a way to the end hub.

Author Tamilselvan L, and Sankaranarayanan V [13], has formulated a Time-based Threshold Detection framework which is dependent upon an increase of the first AODV directing convention. This framework is evaluating clock in the Timer Expired Table to gather the further ask for from different hubs in the wake of gaining the first ask. It will gather the bundle's arrangement number and gained time in a Collect Route Reply Table (CRRT), including the timeout worth dependent upon the accepted time of the starting course ask for, judging the course have a place with suitable or not dependent upon the above limit esteem.

Author Payal N Raj, and Prashant B Swadas [14], has proposed DPRAODV (discovering, getting away and reactive AODV) to forestall barrier against dark gap by educating helper hubs in the system. It utilizes ordinary AODV where a hub gets the Route answer (RREP) parcel which at first checks the quality of succession number in its directing table. The RREP is secured assuming that its grouping is better to that in the directing table. It then checks if the arrangement number is superior to the limit esteem, and assuming that it is superior to what it is recognized to be the vindictive hub. The worth of the limit quality is redesigned in the time interim; this builds the handling of versatile hub.

Lee, B.han, and M.shin [15], provides a scheme that strengthens robustness of routing information in ad hoc networks. The course affirmation demand (CREQ) and course affirmation answer (CREP) to go around the dark opening assault. The middle of the road hub notwithstanding exchanging RREPs to the source hub moreover sends CREQs to its next-jump hub towards the end hub. The following jump hub on conveyance of a CREQ searches up its save for a course to the goal. Assuming that a course is available, it sends the CREP to the source. On gaining the CREP, the source hub looks at the way in RREP and the one in CREP. In the event that both are indistinguishable the source hub telecasts the course to be right. Though in this proposal black hole attack is not determined if two consecutive nodes work in agreement.

M.a.shurman, S.m.yoo, and S.park [16], answers for the dark gap issue have proposed the source hub to stick around until the entry of a RREP bundle from above two hubs. On receipt of different Rreps, the source hub checks around a basic jump. Assuming that no less than one bounce is basic, the source hub pronounces that the course is secure. The burden is the foreword of a period defer because of the hold up until the entry of numerous Rreps.

Satoshi Kurosawa, Hidehisa Nakayam, Nei Katoabbas Jamalipour, and Yoshiaki Nemoto in [17]gave a strategy to recognize and anticipate dark gap strike by telling different hubs in the system of the episode are found. To beat the tests, there is a necessity to fabricate a multi wall security result that attains both expansive insurance and attractive system execution. It likewise gives clarification about ANT NET, where ACO framework and pseudo code of it has been proposed.

Nisha P John, and Ashly Thomas in [18] exhibited the existing answers for dark opening strike on AODV convention. The paper states that a definitive objective of the security answers for remote systems is to accomplish security objectives that incorporate Confidentiality, Availability, and Non-disavowal, uprightness, verification to versatile clients. Dark gap strike is around the serious security dangers in specially appointed systems which could be effectively utilized by abusing powerlessness of on- interest steering conventions, for example, Ad-Hoc on Demand separation vector (AODV).

Ms Monika Y. Dangore, and Mr Santosh S. Sambare in [19] proposes an endeavor to comprehend the conceivable answers for Black opening ambush with different procedures proposed prior. The essential test in building a MANET is furnishing every gadget to consistently keep up the data needed to appropriately course movement.

AODV (Ad-hoc On-interest Distance Vector) is a circle free directing convention for specially appointed systems. It is wanted to be beginning toward oneself in a climate of versatile hubs, recognizing a mixed bag of system practices.

Arnab Mitra,rajib Ghosh, Apurba Chakraborty,and Debleena Srivastva in [20] provides details regarding Alive and Black Hole hub identification assuming that it exists in any Mobile impromptu systems (Manets). To manage this steering wreckage, an Artificial Neural Network (ANN) based computerized Black Hole hub location strategy has been proposed, which is fit for identifying the presence of Black gap node(s) in the MANET and accordingly serves to minimize the crush up in solid directing method.

Puneet Kansal, Nishant Prabhat, and Amit Rathee in [21] depicts that the dark gap assault in remote Ad Hoc activity between victimized person hub and the vindictive hub then system is real issue that needs skilled results. The dark opening assault makes misjudging by presenting blame in steering data that leads the hub to select wrong way consequently information lose happen. Specially appointed system presents customary blunder redress in steering data that leads the hub to select right way subsequently secure transmission will happen between source and objective.

4. Conclusion

Mobile ad hoc network (MANET) is a set of mobile hosts without the required involvement of any existing infrastructure or centralized access point (base station). Security is very important feature that could determine the success and ample deployment of MANET. Many attacks have been identified and the countermeasures against the most popular attack i.e. Black hole Attack under which performance and efficiency of network decreases considerably by malicious nodes. Under black hole attack, a malicious node overcomes a destination node by sending a wrong route reply packet to a source node that describes a route discovery. By doing this, the malicious node can withdraw the traffic from the source node. So security measures are necessary to protect the network from such dangerous attacks. Thus it can be said that the success of the network depends upon the level of security it ensures.

REFERENCES

[1] *MANET*.Available:www.techterms.com/

[2] *Mobile Ad Hoc Networks (MANETs).* Available: http://www.antd.nist.gov/

[3] Aarti, Dr. S. S. Tyagi, 2013, Study of MANET: Characteristics, Challenges, Application and Security Attacks, *IJARCSS*, vol. 3, pp. 252-257.

[4] Piyushmittalin.Security-in-mobile-ad-hoc-networks.Available:www.slideshare.net/

[5] manet-mobile-ad-hoc-network characteristics-and-features.Available: www.eexploria.com/

[6] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, 2011, A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks, *Journal of Computing*, vol. 3, pp. 41-48.

[7] Wenjia Li, Anupam Joshi , and Tim Finin, 2011, SAT: an SVM – based Automated Trust Management System for Mobile Ad- hoc Networks, *Military Communications Conference IEEE*, pp. 1102-1107.

[8] Bo-Cang Peng and Chiu-Kuo Liang, 2006, Prevention techniques for flooding attack in Ad Hoc Networks, *IEEE.*

[9] Douglas S. J. De Couto, Daniel Aguayo, John Bicket and Robert Morris., 2003, A High-Throughput Path Metric for Multi-Hop Wireless routing, *ACM Mobicom*, pp. 419-434.

[10] D.M. Shila and T. Anjali, 2008, Defending selective forwarding attacks in WMNs, *IEEE International Conference on Electro/Information Technology*, pp. 96-101.

[11] X.P. Gao and W. Chen, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks[C]", IFIP International Conference on Network and Parallel Computing Workshops, 2007, 209-214.

[12] Hongmei Deng, Wei Li, and Dharma P.Agrawal, 2002, Routing Security in Wireless Ad Hoc Network, IEEE *Communications Magzine*, vol. 40, pp. 70-75.

[13] Tamilselvan L and Sankaranarayanan V, 2007, Prevention of Black hole Attack in MANET, *2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, pp. 27-30.

[14] Payal N. Raj and Prashant B. Swadas, 2009, DPRAODV: A dynamic learning system against black hole attack in AODV based Manet, *International Journal of Computer Science Issues (IJCSI)*, vol. 2, pp: 54-59.

[15] S.Lee, B.Han, and M.Shin, 2002, Robust Routing in Wireless Ad Hoc Networks, *Proceedings of International. Conference on Parallel Processing Workshop*, pp. 73-78.

[16] M.A.Shurman, S.M.Yoo, and S.Park, 2004, Black Hole Attack in Mobile Ad Hoc Networks, *ACM Southeast Regional Conference*, pp. 96-97.

[17] Satoshi Kurosawa,Hidehisa Nakayam, Nei KatoAbbas Jamalipour and Yoshiaki Nemoto, 2007, Detecting Black hole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method, *International Journal of Network Security*, vol. 5, pp. 338-346.

[18] Nisha P John, Ashly Thomas, 2012, Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Networks - A Review, *International Journal of Innovative Research and Development 1*, pp.232-245.

[19] Monika Y. Dangore, Mr Santosh S. Sambare, 2013, A Survey on Detection of Black hole Attack Using AODV Protocol in MANET, *International Journal on Recent and Innovation Trends in Computing and Communication 1*, pp. 55-61.

[20] Arnab Mitra,Rajib Ghosh, Apurba Chakraborty,Debleena Srivastva, 2013, An Alternative Approach to Detect Presence of Black Hole Nodes in Mobile Ad-Hoc Network Using Artificial Neural Network.

[21] Puneet Kansal, Nishant Prabhat, Amit Rathee, 2013, Black hole attack in MANETs, *International Journal 3.*

A Brief Author Biography

Harmanpreet Kaur received the B.Tech with Hons degree in Computer Science and Engineering from the Lovely Professional University, Phagwara in 2012. She is working toward the M.Tech degree in Department of Computer Science and Engineering at DAV Institute of Engineering & Technology, Jalandhar under Punjab Technical University. Her research interests include networking, web designing, MANETs and security.

P.S.Mann is currently working as Assistant Professor at DAV Institute of Engineering & Technology, Jalandhar. He is B.Tech with Hons, M.Tech and has experience of 8 years in teaching. His research interest includes Computer Networks, Wireless Communication, Cloud Computing. He has published more than 25 papers in International Journals, 01 in National Journals, 01 in International Conferences and 07 in National Conferences. He is Life Member of Punjab Academy of Sciences and Computer Society of India.