Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.710 – 717

RESEARCH ARTICLE

A Honey-Pot Server Based Blackhole Attack Detection in AODV Based MANETs

[1]D.Nithya Priyadharsini MCA., [2]L.Devi MCA., M.Phil.
[1]M.Phil. Research Scholar in Computer Science
[2]Associate Professor in Computer Science
[1.2]Muthayammal College of Arts and Science, Rasipuram

ABSTRACT: In this paper learn the Ad-hoc networks be exposed to black hole attack. Black hole attacker drops each incoming reasonable packet to make use of on-demand direction-finding as well as data escape in ad-hoc network. Black hole attacker exploits on-demand routing by falling route request packets. It drops route request packet instead of forwarding it and send route reply as if it has a valid route to target. As an outcome, all data from source will be delivered towards black hole attacker. In this paper, we have proposed a honey-pot server based approach to on-demand routing to defend black hole attacker depending on this model with different level of estimation. In our approach, Black hole attackers are identified and isolated on the context of data forwarding. Analysis and simulation results justifies our proposal against black hole attack for AODV, on-demand routing protocol in the form of AODV against Black hole attack and find the times based detection system.
Index Term: Short route Black hole Attacks, Time Based Detection, Manet

1. INTRODUTION

The mobile nodes which are usually MANETs have constraint due to secure MANETs are strong. The main four constraints are limited central processing unit (CPU) power; time based detection, and node mobility which produces latency in convergence of the network. These constraints present the following security issues: signal jamming, denial-of-service, battery exhaustion, authenticity, integrity, and confidentiality [4]. These five attributes of network of attack detection along with the constraints MANETs make it challenging to design a protocol that fulfills all the requirements. However, this is not the only attack against MANETs. MANETs are susceptible to routing protocol attacks and route disruption attacks. The threats that are unique to MANETs and are as follows: Worm-hole attack, Greyhole attack, Sinkhole attack, and Sybil attack [5-7]. Black-hole attack is a type of active attack that exploits the RREP feature of AODV. These attacks involve some modification of the data stream or the creation of a false stream [5]. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. Hence, a source node updates its routing table for the new route to the particular destination node and discards any other messages from other neighboring nodes or even from the actual destination node. Once a source node saves a route, it starts sending buffered data packets to a hateful node hoping they will be

forwarded to a destination node. Nevertheless, a hateful node (performing a black-hole attack) drops all data packets rather than forward them on. A in depth learn of the various attacks can be seen in [4, 5]. So far we know that black-hole attack is a DoS attack that disrupts the services of routing layer by exploiting the route discovery process of AODV in MANETs. Over the past years, researches have been carried out to show the adverse effect of black-hole harass in MANETs. In order to handle black-hole attack, research has been accepted to increase method or totally new protocol..

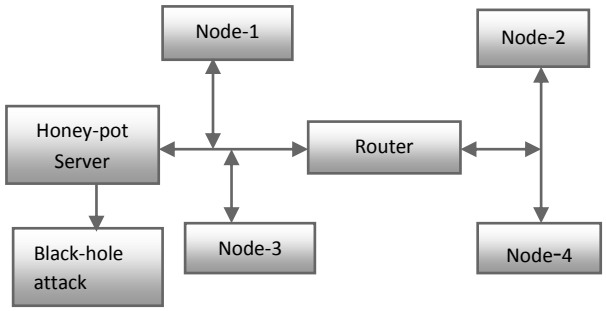
1.1 Black hole Solution

If an attacker truly wanted to compromise your LAN and Manet security, the most effective approach would be to send random unauthenticated packets to every Manet station in the network. This exploit can be easily achieved by purchasing hardware off the shelf from an electronics retailer and downloading free software from the internet. In some cases, it is simply impossible to defend against Blackhole as an experienced attacker may have the ability to flood all available network frequencies.

If the major concern relates to malicious Blackhole, an intrusion prevention and detection system may be your best option. At the bare minimum, this type of system should be able to detect the presence of an RPA (Rogue Access Point) or any authorized client device in your Manet network. More advanced systems can prevent unauthorized clients from accessing the system, alter configurations to maintain network performance in the presence of an attack, blacklist certain threats and pinpoint the physical location of a rogue device to enable faster containment.

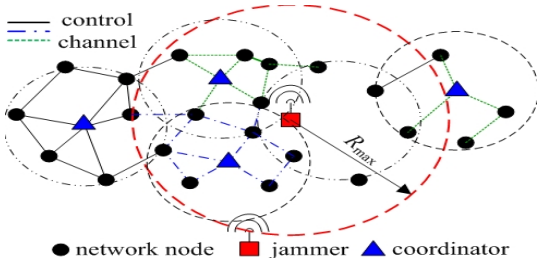
2. RELATED WORK

In modern era the accommodations provided by the 802.11 based Manet access network led to its deployment in various sectors such as defense, consumer and industrial sector. Openness of Manet network makes it vulnerable to various types of attacks. Out of various types of attacks, Denial-of-service (DoS) attack is one of the most troublesome threats which prevent legitimate users from accessing the network. It is executed in many ways such as intentional interference or Blackhole. Blackhole is one of many exploits used compromise the Manet environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. If an attacker truly wanted to compromise your LAN and Manet security, the most effective approach would be to send random unauthenticated packets to every Manet station in the network. To minimize the impact of an unintentional disruption, it is important to identify its presence. Blackhole makes itself known at the physical layer of the network, more commonly known as the MAC (Media Access Control) layer. The increased noise floor results in a faltered noiseto- signal ratio, which will be indicated at the client. It may also be measurable from the access point where network management features should able to effectively report noise floor levels that exceed a predetermined threshold. From there the access points must be dynamically reconfigured to transmit channel in reaction to the disruption as identified by changes at the physical layer.



2.1 DETECTION OF BLACKHOLE

The network employs a monitoring mechanism for detecting potential malicious activity by a Blackhole. The monitoring mechanism consists of the following: (i) determination of a subset of nodes *M* that will act as network monitors, and (ii) employment of a detection algorithm at each monitor node. The assignment of the role of monitor to a node can be affected by energy limitations and detection performance specifications. In this work, we fix *M* and formulate optimization problems for one or more monitor nodes. We now fix attention to detection at one monitor node. First, we define the quantity to be observed at each monitor node. In our case, the readily available metric is probability of collision that a monitor node experiences, namely the percentage of packets that are erroneously received. During normal network operation, and in the absence of a Black hole, we consider a large enough training period in which the monitor node "learns" the percentage of collisions it experiences as the long-term average of the ratio of number of slots in which there was a collision over total number of slots of the training period. Assume now the network operates in the open after the training period and fix attention to a time window much smaller than the training period. An increased percentage of collisions over this time window compared to the learned long-term average may be an indication of an ongoing Blackhole attack or only a temporary increase of percentage of collisions compared to the average during normal network operation. A detection algorithm takes observation samples obtained at the monitor node (i.e, collision or not collision) and decides whether there exists an attack. On one hand, the observation window should be small enough, such that the attack is detected on time and appropriate countermeasures are initiated. On the other hand, this window should be sufficiently large, such that the chance of a false alarm notification is minimized.



2.2 Monitoring and detecting

A honey pot is a deception trap, designed to entice an attacker into attempting to compromise the information systems in an organization. If deployed correctly, a honey pot can serve as an early-warning and advanced security surveillance tool, minimizing the risks from attacks on IT systems and networks. Honey pots can also analyses the ways in which attackers try to compromise an information system, providing valuable insight into potential system loopholes

2.3 Surveillance tool

Think for a moment about what information you routinely supply to complete strangers. Cash a check and you must provide your name, address and phone number long with some form of "acceptable" identification. The cover is to protect the organization accepting the check and if that we are all that it was used for there might be no objection. However, what happens to the information supplied? Is it ever used for any but the purpose stated? For every credit card transaction, much detailed information is transcribed and stored for later use (such as time, date of purchase, items purchases, location of purchase, amount of purchase and much more). If it were only used for billing purposes there might be no objection.

3. Performance Evaluation

In this section, the evaluation of the proposed scheme in terms of end-to-end delay and throughput is described. Minimizing the risks from attacks on IT systems and networks. Honey pots can also analyse the ways in which attackers try to compromise an information system, providing valuable insight into potential system loopholes. This article provides a brief explanation of honeypots, and how they can be deployed to enhance organizational and enterprise security across critical systems and networks.

4. SIMULATION RESULT

4.1 REAL-TIME PACKET CLASSIFICATION

In this section, we explain how the opponent can classify packets in real time, previous to the packet broadcast is accomplished. Once a packet is classified, the adversary may choose to jam it depending on his strategy. Consider the generic communication system depicted. At the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the Manet channel. At the receiver, the signal is demodulated, interleaved, and decoded, to recover the original packet m.

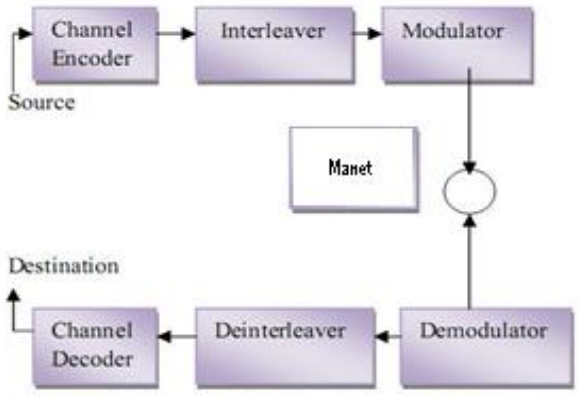


Fig. A general communication system diagram

The adversary's aptitude in classifying a packet m depends on the accomplishment of the blocks in Fig. 2. The channel indoctrination block expands the innovative bit sequence m, adding essential redundancy for defensive m against channel errors. For example, an α/β-block code may protect m from up to e errors per block. Alternatively, a α/β-rate convolution encoder with a constraint length of Lmax and a free distance of e bits provides similar protection. For our purposes, we assume that the rate of the encoder is α/β. At the next block, interleaving is applied to protect m from burst errors. For simplicity, we consider a block interleaver that is defined by a matrix Ad×_ 1. The de-interleaver is simply the transpose of A. Finally, the digital modulator maps the received bit stream to symbols of length q, and modulates them into suitable waveforms for transmission over the Manet channel. Typical modulation techniques include OFDM, BPSK,-QAM, and CCK.

4.2. Proposed Detection Algorithm

Step 1

The sender and receiver change channels in order to stay away from the Blackhole, in channel hoping technique.

Step 2

The pair-wise shared key KS is used for creating a channel key KCh = EKS(1) , which generates a pseudorandom channel sequence

$$Chs = \{EKS(i) \bmod Ch\},\ i \geq 0,$$

Where, Ch is the number of channels available in the band, cmessage mi is transmitted on channel Chi, (unknown to any c but the two parties involved.)

Step 3

Using packet fragmentation technique, the packets are break into fragments to be transmitted separately on different channels and with different SFD (start of frame delimeter). The last fragment contains a frame check sequence FCS for the entire payload.

Step 4

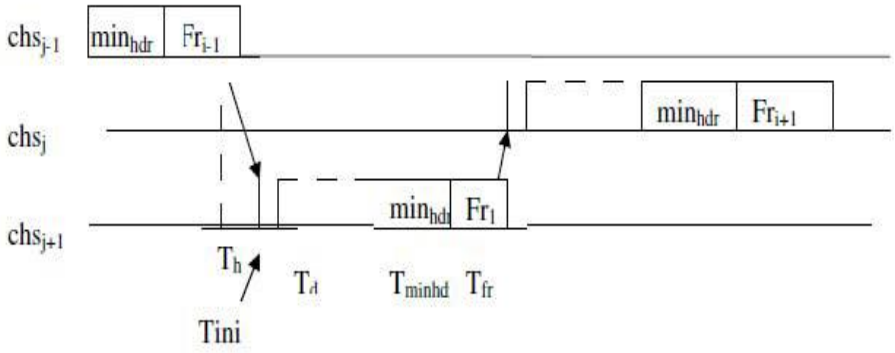


Fig. Packet fragmentation technique

The above figure shows the way in which fragments are transmitted. To transmit fragment Fri, the sender hops to Chi, fills the transmit FIFO with Fri, sets SFD to Si, and issues the transmit command.

Step 5

The time to transmit the fragment is Tfrag = Th + T ini + Td + Tminhdr + Tfr

Step 6

If the fragments are short, the attacker's Black hole message does not start till the sender has finished transmitting and hopped to another channel.

Step 7

In the Pulse Blackhole attack, the Blackhole remains on a single channel, hoping to disrupt any fragment that may be transmitted. As packets cannot be detected quickly enough for selective Black hole, the attacker transmits blindly in short pulses. The black hole pulses must occur no less frequently than Tminhdr + Tfr to prevent any fragments from slipping through.

Step 8

The forward ants (FA) explore the network to collect the Black hole's information on each channel. It keeps collecting the attackers' data if any and moves forward though channels. When the FA reaches the end of the channel, it is deallocated and the backward ant (BA) inherits the stack contained in the FA.

Step 9

The BA is sent out on high priority queue. The backward ants retrace the path of the FA and utilize this information to update the data structures periodically.

Step 10

As it reaches the source, the data collected is verified

Which channel there is prevalence of attacker long time and those are omitted. Simultaneously the forward ants are sent through other channels which are not detected before for attacks.

Step 11

The FAs either unicast or broadcast at each node depending on the availability of the channel information for end of the channel.

Step 12

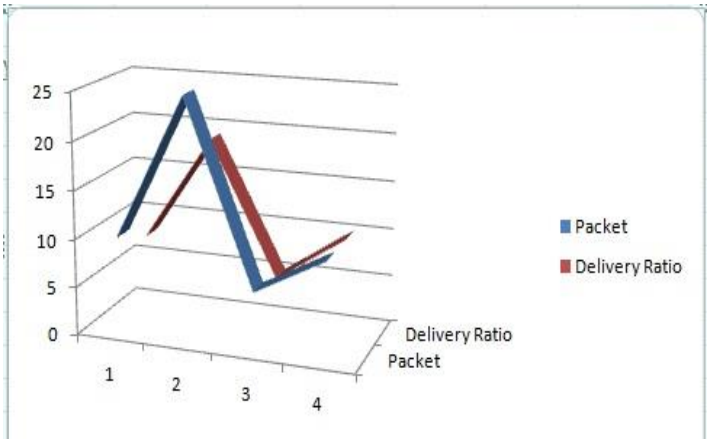
If the channel information is available, the ants randomly choose the next hop. This scheme helps limit the channel maintenance overhead. If the pheromone information is available at the channel i , then the channel probability P (Chi, j,d) of choosing neighbor channel j as the next hop for last.

$$P(Ch_{i,j,d}) = \frac{[\sigma_{i,j,d}]^{\alpha}[\lambda_{i,j}]^{\beta}}{\sum_{l \in N_i}[\sigma_{i,l,d}]^{\alpha}[\lambda_{i,l}]^{\beta}}$$

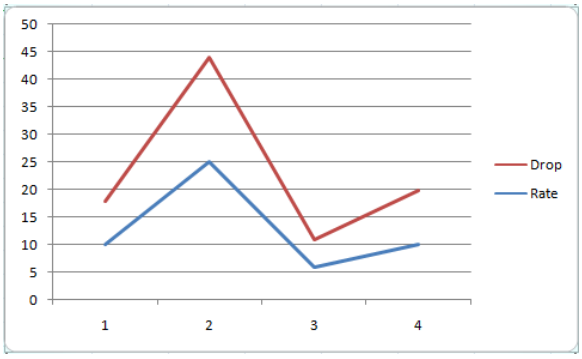
4.3. Performance Metrics

The proposed detection algorithm Defense Technique (SBDT) is compared with the DEEJAM detection technique [8]. The performance is evaluated mainly, according to the following metrics.

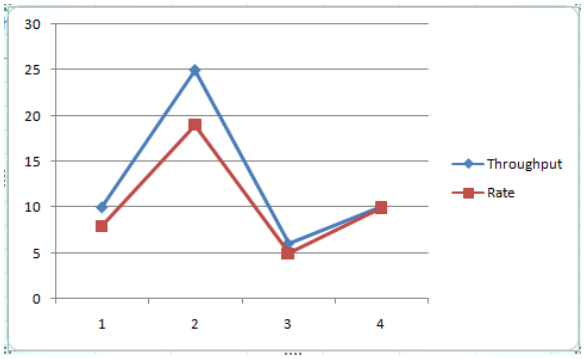
- Aggregated Throughput
- Packet Delivery Ratio
- Packet Drop



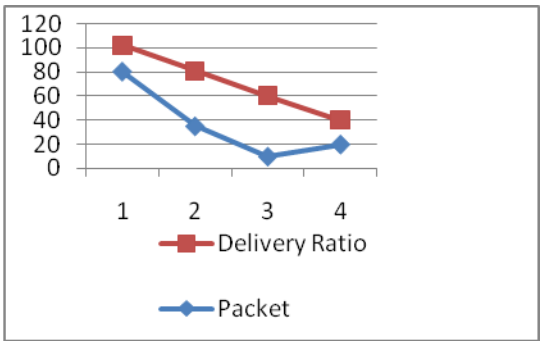
Packet Delivery Ratio



Rate vs Packet dropped



Rate and Throughput



Time and Delivery

5. CONCLUSION

They are simple and easy to deploy and maintain. In addition, the limited emulation available and/or allowed on interaction honey pots reduces the potential risks brought about using them in the field. However, with interaction honey pots, unlimited information can be obtained, and it is possible that experienced attackers will not come to recognize a honey pot when they come across one. We estimate the collision of alert Black hole attacks on network protocols such as TCP and routing. Our findings show that a selective Black hole can widely impact performance with very low effort. We developed schemes that alter a Black hole to a unsystematic single by prevent real-time packet categorization.

REFERENCES

1. Black hole and Sensing of Encrypted Manet Ad Hoc Networks. Timothy X Brown Jesse E. James Amita Sethi University.
2. Detection and Prevention of various types of Blackhole Attacks in Manet Networks. Mr. Pushphas Chaturvedi Mr. Kunal Gupta Dept. Of Computer Science Dept. Of Computer science Amity University Amity University.
3. Introduction to Blackhole Attacks and Prevention Techniques using Honeypots in Manet Networks. Neha Thakur Dept. of Software Engineering SRM University Aruna Sankaralingam Dept. of Software Engineering SRM University Chennai, India.
4. Blackhole Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks. Kwangsung Ju and Kwangsue Chung Department of Communications Engineering Kwangwoon University, Seoul, Korea ksju@cclab.kw.ac.kr, kchung@kw.ac.kr.
5. A Swarm Based Defense Technique for Blackhole Attacks in Manet Sensor Networks. S. Periyanayagi and V. Sumathy.

6. Packet-Hiding Methods for Preventing Selective Blackhole Attacks. Alejandro Proa˜no and Loukas Lazos Dept. of Electrical and Computer Engineering, University of Arizona, Tucson, AZ, USA E-mail :{aaproano, llazos}@ece.arizona.edu.
7. T. X. Brown, J. E. James, and A. Sethi. Blackhole and sensing of encrypted Manet ad hoc networks. In Proceedings of MobiHoc, pages 120–130, 2006.
8. M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormhole-based antiBlackhole techniques in sensor networks. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.
9. A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel Blackhole: Resilience and identification of raitors. In Proceedings of ISIT, 2007.
10. T. Dempsey, G. Sahin, Y. Morton, and C. Hopper. Intelligent sensing and classification in ad hoc networks: a case study. Aerospace and Electronic Systems Magazine, IEEE, 24(8):23–30, August 2009.
11. Y. Desmedt. Broadcast anti-Blackhole systems. Computer Networks, 35(2-3):223–236, February 2001.
12. K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.

