A Proximity Set Method Based Learn System Against Black-Hole Attack Inside MANET

Nedumaran Arappali[1], Abdul Kerim.S[2], Tedros Salih Abdu[3], Tegegne Ayalew[4]
Department of Electrical & Computer Engineering
Lecturer's,, Kombolcha Institute of Technology,Wollo University, Ethiopia, Africa

Abstract-*In this work, we address the problem of selective Blackhole attacks in Manet networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. We illustrate the advantages of selective Black hole in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing. We show that selective Blackhole attacks can be launched by a proximity set method based learning system. To mitigate these attacks, we develop three schemes that this method combining with cryptographic primitives with physical-layer attributes. We analyze the security of our methods and evaluate their computational and communication overhead.*

Keywords-Selective Black hole Attacks, Packet Hiding, TCP, Manet Network.

I. INTRODUCTION

Ad hoc networks are envisioned as playing a significant role in mission critical communication for the military utilities, and industry. An adversary may attempt to attack a victim ad hoc network to prevent some or all victim communication. Such denial-of-service (DoS) attacks have been considered in ad hoc Manet networks at several levels. A number of researchers have considered DoS where the attackers are internal participants in the victim ad hoc network (see e.g. 1). Ad hoc networks require the cooperation of peer nodes for their operation and are especially susceptible to such peer-based attacks. In this paper we consider encrypted victim networks in which the entire packet including headers and payload are encrypted and thus the attacker cannot directly manipulate any of the victim communication. In this case, the attacker must resort to external physical-layer-based DoS, also known as Blackhole.

Since RF (radio frequency) is essentially an open medium, Blackhole can be a huge problem for Manet networks. 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. A knowledgeable attacker with the right tools can easily jam the 2.4 GHz frequency in a way that drops the signal to a level where the Manet network cans no longer function. The complexity of Blackhole is the fact that it may not be caused intentionally, as other forms of Manet technology are relying on the 2.4 GHz frequency as well. Some widely used consumer products include cordless phones, Bluetooth-enabled devices and baby monitors, all capable of disrupting the signal of a Manet network and faltering traffic. The issue of Blackhole mostly relates to older Manet local area networks as they are not fully equipped to make the adaptation to numerous types of interference. These networks typically call for an administrator to manually adjust each access point through trial and error. To avoid this daunting task, the best practice is to invest into a newer WLAN system. These environments offer real-time RF management features capable of identifying and adapting to unintentional interference.

Blackhole Solution

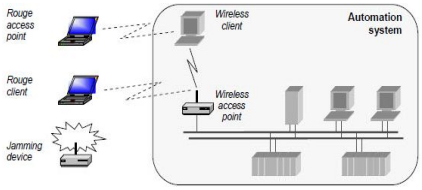
If an attacker truly wanted to compromise your LAN and Manet security, the most effective approach would be to send random unauthenticated packets to every Manet station in the network. This exploit can be easily achieved by purchasing hardware off the shelf from an electronics retailer and downloading 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.

II. RELATED WORK

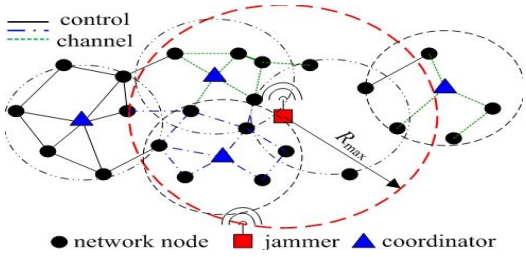
In modern era the accommodations provided by the 802.11 based Manet access network led to its deployment in

various sectors such as defence, 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 threat 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.



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 Blackhole , 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.



Blackhole Type

Therefore, Blackhole is an entity who is purposefully trying to interfere with transmission and reception of message across the Manet channel. Recently, several Blackhole strategies have been introduced. Later, Blackhole s were categorized into four models. They are

Constant Blackhole

In this model, Blackhole continuously emits RF signals and it transmits random bits of data to channel. It does not follow any MAC layer etiquette. Being onstant to the transfer it does not wait for channel to become an idle.

Reactive Blackhole

In this model, Blackhole will stay quite when the channel is idle. As soon as it senses activity on channel, it starts transmitting signal. In order to sense the channel Blackhole is ON and should not consume energy.

To mitigate Blackhole attacks many hiding schemes wereused. These are

- Strong hiding commitment scheme
- Cryptographic puzzle base scheme

- All-or-nothing transmission

Deceptive Blackhole

In this model, Blackhole constantly injects series packets to the channel without any gap between subsequent transmissions. It also broadcasts fabricated messages and reply old ones. Blackhole will pass reambles out to the network and just check the preamble and remain silent.

Random Blackhole

In this model, Blackhole alternates between period of continuous Blackhole and inactivity. After Blackhole for t1 units of time, it stops emitting radio signals and enter into sleep mode. The Blackhole after sleeping for t2 units of time wakes up and resumes Blackhole . Both time t1 and t2 is either random or fixed.

III. PERFORMANCE EVALUATION

In this section, the evaluation of the proposed scheme in terms of end-to-end delay and throughput is described. Simulations have been conducted using OPNET Modeler 16.0 [9]. We compare the proposed scheme with jammed area mapping scheme [4]. In order to implement proposed robust rate adaptation scheme, we modify IEEE 802.11 DCF (Distributed Coordination Function) scheme in OPNET Modeler. The simulation parameters are summarized in Table 1

Simulation Result

PARAMETER	VALUE
Simulation area	12 Km × 12Km
Transmission rage	9 Km
Traffic model	CBR
Transmission data rate	2 Mbps
Simulation time	10000 second
Signal strength threshold	-79 dBm
PDR threshold	79 %

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, deinterleaved, and decoded, to recover the original packet m.

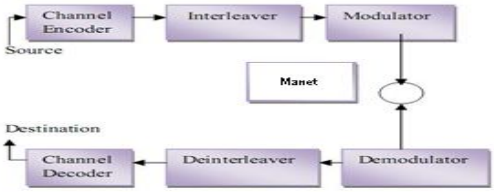


Fig. 2. A general communication system diagram.

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, an 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

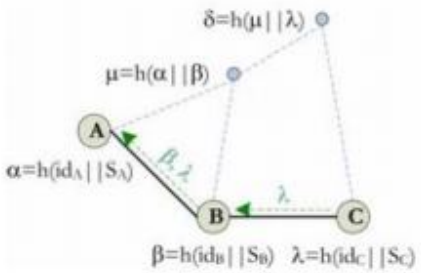


Fig. 3. Back whole attack detection

Source node compares this value with prior saved hash value of this route in its memory and if any differences found, it then informs other nodes about maliciousness of this route. Difference between saved value and new value shows

that one node may drops RREQ packets and does not send packets to destination that does not have correct value. This method can also find cooperative black hole attacks.

Advantages

- In this method all nodes do not monitor each other so.
- A lot of energy is not consumed for monitoring. Detecting cooperative black hole attacks is another.
- Benefit of this scheme.

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 anycbut 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

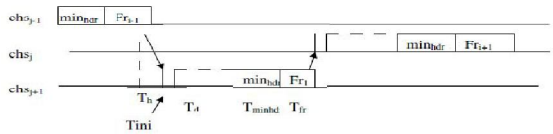


Fig. 2. Packet fragmentation technique

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 Blackhole 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 Blackhole , the attacker transmits blindly in short pulses. The Blackhole 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 Blackhole '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 theFA.

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.

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

IV. 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

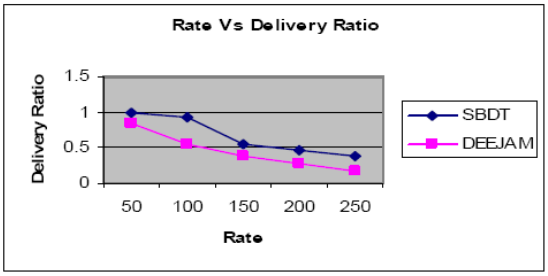


Fig. 2. Rate Vs packet delivery ratio

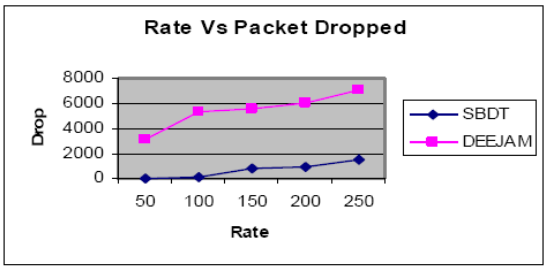


Fig. 3. Rate Vs packet dropped

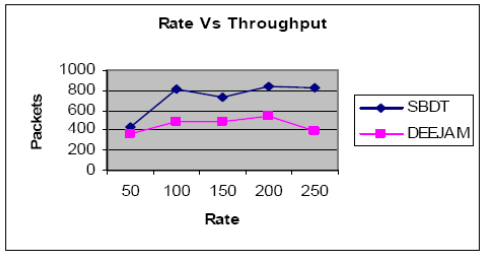


Fig. 4. Rate Vs throughput

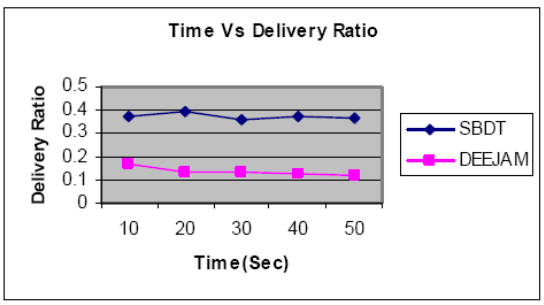


Fig. 5. Time Vs packet delivery ratio

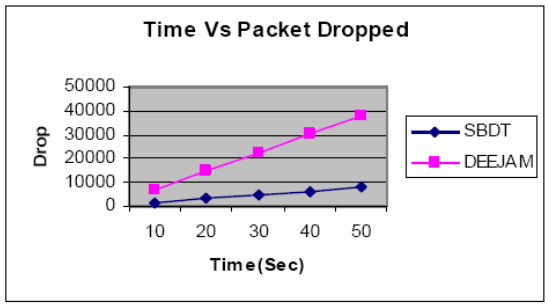


Fig. 6. Time Vs packet dropped

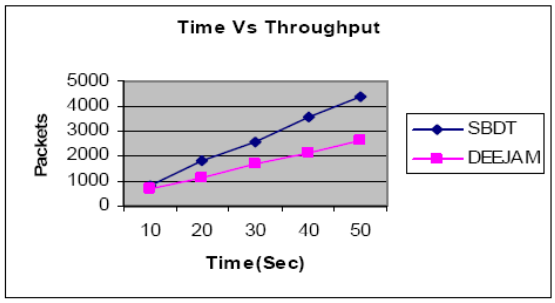


Fig. 7. Time Vs throughput

V. CONCLUSION

An exploit can be either an information-gathering probe or an attack to compromise, disable, or harm a network or network resource. In some cases, the distinction between the two objectives of an exploit can be unclear. For example, a barrage of TCP SYN segments might be an IP address sweep with the intent of triggering responses from active hosts, or it might be a attack with the intent of overwhelming a network so that it can no longer function properly. Furthermore, because an attacker usually precedes an attack by performing reconnaissance on the target, we can consider information-gathering efforts as a precursor to an impending attack that is, they constitute the first stage of an attack. Thus, the term exploit encompasses both reconnaissance and attack activities, and the distinction between the two is not always clear. We evaluated the impact of selective Blackhole attacks on network protocols such as TCP and routing. Our findings show that a selective Blackhole can significantly impact performance with very low effort. We developed three schemes that transform a selective Blackhole to a random one by preventing real-time packet classification.

REFERENCES

[1] Blackhole 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.