Volume 5, Issue 4, April 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Intrusion Detection System Using EAACK for DOS and Gray Hole Attacks in MANET

Prathamesh Saswade*, **Mamta Jangira, Himanshi Raina, Asst. Prof. Rohini Pise**

Department of Information technology Pimpri Chinchwad College of Engineering,
Pune, Maharashtra, India

Abstract: The development to wireless system from wired system has been an overall example in the late decades. In all the wireless system, Mobile Ad hoc Network (MANET) is the most discriminating and exceptional applications. Nodes compare particularly with each other when they are both inside the same correspondence range. Else, they depend upon their neighbours to exchange messages. The arranging toward oneself limit of nodes in MANET made it conspicuous among basic mission applications like military use or emergency recuperation. In this paper, we proposed intrusion detection framework named Enhanced Adaptive Acknowledgment (EAACK) remarkably expected for MANETs. We have utilized two methods via, IP header utilization, encoding schemes. Here we analyse and detect two types of attack such as, DOS Attack, Gray Hole attack. It helps for intrusion detection. Examined to contemporary techniques, EAACK shows higher malicious detection rates in particular circumstances while does not incredibly impact the system performance. It detects both the attacks successfully.

Keywords: Enhanced Adaptive Acknowledgment (EAACK), Mobile Ad hoc Network (MANET); Intrusion Detection System (IDS), DOS (Denial of Service).

I. Introduction

Wireless networks are favoured till its development in view of their scalability and mobility. Referring to the upgraded innovation and decreased costs, remote frameworks have expanded altogether more inclination over wired frameworks in the earlier decades. By definition, Mobile Ad hoc Network (MANET) is a social occasion of adaptable nodes outfitted with both a wireless transmitter and a recipient that relate with each other through bidirectional remote associations either direct or by suggestion. Modern remote access to and control by method for remote frameworks are getting the opportunity to be more standard these days [1]. One of the real purposes of enthusiasm of remote frameworks is its ability to allow data correspondence between diverse gatherings and still keep up their mobility. In any case, this correspondence is restricted to the extent of transmitters. This suggests that two nodes can't relate with each other when the partition between the two nodes is past the correspondence scope they could call their own. MANET handles this issue by permitting intermediate parties to hand-off data transmissions. This is expert by secluding MANET into two sorts of frameworks, to be particular, single-hop and multihop. In a single hop compose; all nodes inside the same radio degree correspond particularly with each other. Then again, in a multihop framework, nodes rely on upon other transitional nodes to transmit if the end of the destination node is out of their radio range. MANET is prepared for making a designing toward oneself and keeping up toward oneself up framework without the support of a unified infrastructure, which is frequently infeasible in separating mission applications like military clash or crisis recovery. Irrelevant design and fast development make MANET arranged to be used as a part of circumstances in crisis where a structure is possessed or unfeasible to present in circumstances like trademark or human-instigated disaster, military clashes, also therapeutic emergency circumstances [2], [3]. Owing to these special attributes, MANET is getting the opportunity to be all the more extensively executed in the business [4], [5]. On the other hand, considering the way that MANET is acclaimed among separating mission applications, framework security is of essential basics. The open medium and remote assignment of MANET make it weak against distinctive sorts of attacks. For example, due to the nodes non appearance of physical protection, malicious attacker can without a doubt find and node catching to accomplish attacks. In particular, considering the way that most coordinating traditions in MANET acknowledge that every node in the framework carries on accommodatingly with diverse nodes and likely not malicious [6]; assailants can without a doubt deal MANET by embeddings pernicious or no helpful nodes into the system. Besides, as a consequence of MANET's scattered building design and evolving topology, an ordinary incorporated observing framework is not feasible in MANET. In such case, it is critical to make an Intrusion Detection System (IDS) particularly planned for MANETs. In the next section II we are focusing on related work. In section III we focus on implementation work and finally ended with IV section in results.

II. Related Work

Anantvalee and Wu [7] displayed a particularly careful review on contemporary Ids in MANETs. n this section, we for the most part three current approaches, to be specific, Watchdog [8], TWOACK [9], and Adaptive Acknowledgment (AACK) [10].

1) Watchdog: Marti et al. [8] proposed a decision of Watchdog that plans to lookup the throughput of system with vicinity of malicious nodes. To be totally straightforward, the Watchdog arrangement is included two areas, specifically, Watchdog and Pathrater. Watchdog serves as an ID for MANETs. It is careful for perceiving malicious node mischievous in the framework. Watchdog perceives malicious mischievous activities by wantonly listening to its next hop's transmission. If a Watchdog node gets that its next node fails to forward the parcel inside a certain time of time, it constructs its counter of disappointment. At whatever point a nodes counter of failure surpasses a predefined edge, the Watchdog node reports it as acting devilishly. For this circumstance, the Pathrater teams up with the routing protocol to keep up a vital distance from the reported node in future transmission.

2) TWOACK: As for the deficiencies of the Watchdog plan, various masters proposed new systems to disentangle these issues. TWOACK proposed by Liu et al. [11] is a champion amongst the most critical methodologies among them. On the numerous different plans, TWOACK is not one or the other neither an upgrade nor a watchdog-based plan. Intending to reason the impact of beneficiary and limited transmission force issues of Watchdog, TWOACK recognizes misbehaving associations by perceiving every data bundle transmitted over every three persistent hubs along the route from the source to the target. Endless supply of a bundle, each hub along the course is expected to send back an affirmation of parcel to the hub that is two jumps a long way from it down the course. TWOACK is expected to take a shot at routing protocol, for instance, Dynamic Source Routing (DSR) [12].

3) AACK: Based on TWOACK, Sheltami et al. [10] proposed another plan called AACK. Like TWOACK, AACK is in view of acknowledgement system layer arrangement which can be considered as a mix of a plan called TACK (indistinguishable to TWOACK) and an end-to-end arrangement for acknowledgement called Acknowledge (ACK). Stood out from TWOACK, AACK out and out diminished framework overhead while still prepared for keeping up or really surpassing the same framework throughput. To be totally straightforward, a large bit of the current Ids in MANETs grasp a affirmation based plan, including TWOACK and AACK. The limits of such detection plan for all by and large depend on upon the acknowledgement packets. Hereafter, it is dire to guarantee that the affirmation bundles are verifying and in addition substantial. To address this stress, we grasp a mechanized check in our proposed arrangement named Enhanced AACK (EAACK).

III. IMPLEMENTATION DETAILS

A) IP Header Utilization:

FDPM is focused around Ipv4. Possible Ipv6 use of FDPM will incorporate incorporating an augmentation header in Ipv6 packet, which is different with the Ipv4 design. The need of FDPM Ipv6 use needs more research in light of the way that Ipv6 has characteristic security frameworks, for instance, authentication headers to give origin confirmation.

Three fields in the IP header are used for checking; they are Type of Service (TOS), Fragment ID, and Reserved Flag. The TOS field is an 8-bit field that gives an indication of the dynamic parameters. The subtle components of dealing with TOS and specific of TOS qualities can be found in [13]. Along these lines, in FDPM, the TOS field will be used to store the mark if the system framework tradition does not use the TOS document.

Section ID and Reserved Flag are furthermore misused. Given that under 0.25 percent of all Internet action is part [14], Fragment ID can be safely over-stacked without achieving real closeness issues.

The below figure show IP header fields of FDPM

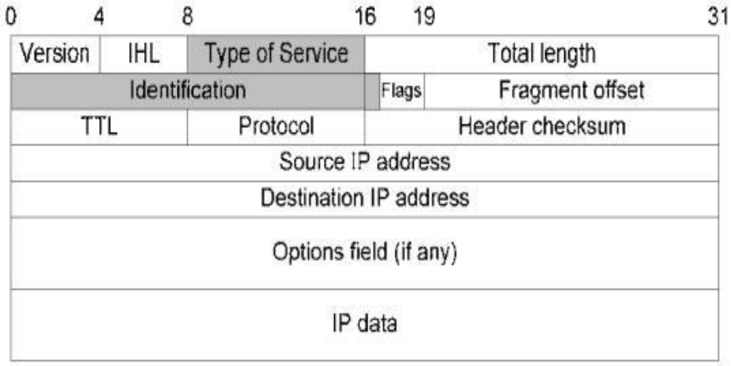


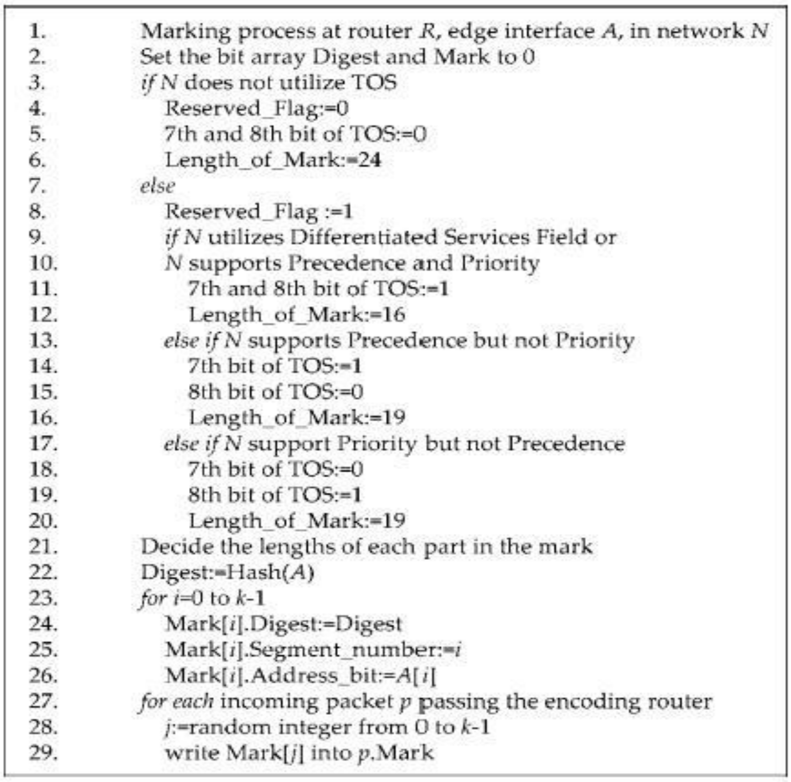
Fig. 1 The IP header fields in FDPM

B) Encoding Scheme:

Before the FDPM mark can be made, the length of the mark must be determined concentrated around the network system traditions convey inside the framework to be guaranteed. According to particular circumstances, the mark length could be 24 bits long at most, 19 bits at center, and 16 bits in any event. Subsequently, the versatile length of the marks realizes three mixed bags of the encoding plan, which are named as FDPM-24, FDPM-19; in addition FDPM-16 in whatever is left of this paper. FDPM encoding arrangement is shown in Fig. 2. The passageway IP area is divided into k parts and set away into parcel named k IP. The cushioning plan is utilized to segment the source IP address just as into k parts.

The fragment number is used to structure the area bits into a right way. The location rundown enables the redoing method to see that the groups being analysed are from the same source. Without this part, the changing strategy can't perceive bundles starting from assorted sources, thusly won't have the ability to take after different IP packets.

The encoding algorithm is exhibited in Fig. 3. In FDPM, preceding the encoding system begins, the length of the mark must be processed. In case the TOS field in the IP parcel is not utilFlag in the header is situated to 0, and the length of mark is situates to 24. Under distinctive circumstances, the length of mark will be 19 or 16, with bit(s) in TOS checked which are important. In case the framework helps TOS Precedence however not TOS Priority, fourth to 6th bits of TOS are utilized for checking; and if the framework helps TOS Priority however not TOS Precedence, first to third bits of TOS are utilized for marking. Sized by the secured framework, the 1-bit reserved.



```
Marking process at router R, edge interface A, in network N
Set the bit array Digest and Mark to 0
if N does not utilize TOS
    Reserved_Flag:=0
    7th and 8th bit of TOS:=0
    Length_of_Mark:=24
else
    Reserved_Flag :=1
    if N utilizes Differentiated Services Field or
    N supports Precedence and Priority
        7th and 8th bit of TOS:=1
        Length_of_Mark:=16
    else if N supports Precedence but not Priority
        7th bit of TOS:=1
        8th bit of TOS:=0
        Length_of_Mark:=19
    else if N support Priority but not Precedence
        7th bit of TOS:=0
        8th bit of TOS:=1
        Length_of_Mark:=19
Decide the lengths of each part in the mark
Digest:=Hash(A)
for i=0 to k-1
    Mark[i].Digest:=Digest
    Mark[i].Segment_number:=i
    Mark[i].Address_bit:=A[i]
for each incoming packet p passing the encoding router
    j:=random integer from 0 to k-1
    write Mark[j] into p.Mark
```

Fig. 2 Algorithm of FDPM encoding scheme

DOS Attack

DOS is most frequently utilized. In such attacks, the objective is to surge the victim with overpowering measures of traffic, and the attacker does not think about receiving reactions to the attacks packets. Packets with spoofed locations are consequently suitable for such attacks. They have extra points of interest for this reason they are more difficult to channel subsequent to every spoofed packets seems to originate from an alternate location, and they hide the genuine source of the attacks. DOS attacks that utilization spoofing commonly arbitrarily pick addresses from the whole IP location space; however more sophisticated spoofing mechanism may avoid unroutable locations or unused parts of the IP address space. The proliferation of large botnets makes spoofing less important DOS attacks, yet attackers normally have spoofing accessible as an tool, in the event that they need to utilize it, so defence against DOS attacks that depend on the validity of the source IP address in a attack packets. Backscatter, a method used to watch disavowal of-administration assault action in the Internet, depends on aggressors' utilization of IP spoofing for its effectiveness.

Steps of the DOS attack are as follows:

Step 1: Initially sender sends the file in chunk size [10 kb]

Step 2: Intermediate node is working as an attacker node

Step 3: Attacker node captures the packets sent by the sender.

Step 4: Attacker node forward the chunks packets to the receiver.

Step 5: Here at receiver side, a threshold rate is provided if the incoming packets are beyond the threshold value the DOS attack is detected.

Gray Hole Attack

In computer networking, a random packet drop attack or gray hole attack is a type of denial-of-service attack in which a router that is supposed to communicate packets instead discards them. This usually occurs from a router becoming cooperation from a number of distinct causes. One cause mentioned in research is through a denial-of-service attack on the router using a known DOS tool. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.

Steps of the Gray Hole attack are as follows:

Step 1: Initially sender sends the file in chunk size [10kb].

Step 2: Intermediate node is working as an attacker node.

Step 3: Attacker node captures and doesn’t forward the packets to save the energy and it acts as a selfish node.

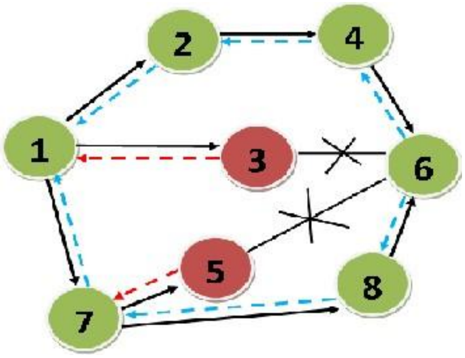


Fig 3. Gray hole attack result.

IV. RESULTS AND DISCUSSION

In the following graph Packet delivery ratio obtained by the gray hole attack detection algorithm is shown. The following graph shows the result obtain before the attack and after the attack. Result with blue line shows the normal data sending or result before the attack and red line shows the result after the attack. In the X-axis represent the malicious node and in Y-axis shows the PDR.

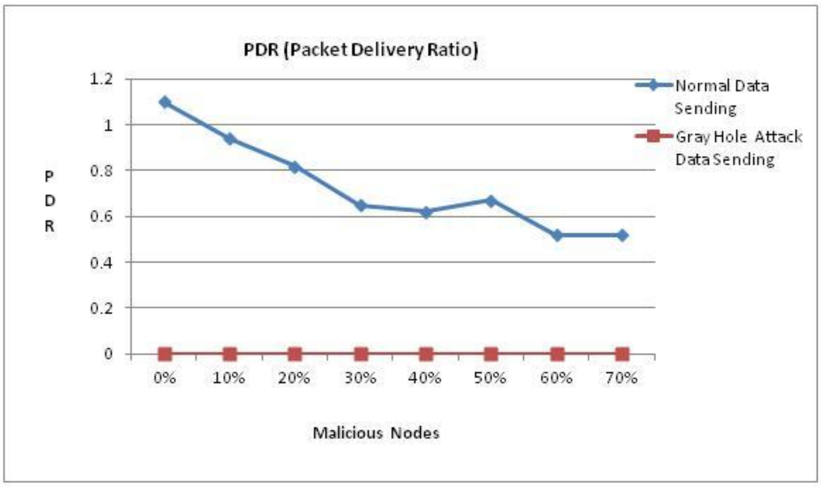


Fig 4. Gray hole attack result.

In the following graph Packet delivery ratio obtained by the DOS attack detection algorithm is shown. The following graph shows the result obtain before the attack and after the attack. Result with blue line shows the normal data sending or result before the attack and red line shows the result after the attack. In the X-axis represent the malicious node and in Y-axis shows the PDR.

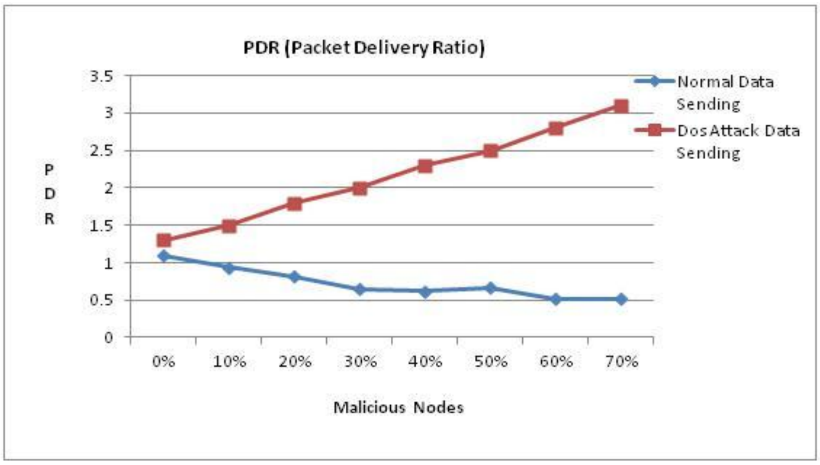


Fig 5. Time graph

V. CONCLUSION

FDPM is suitable for not only for simply taking after sources of DOS attacks but also for DOS recognition. The essential purpose for DOS is to use different attacking sources to attack a defrauded person. Appropriately, any point in the system, if there is a sudden surge in the different packets with the same destination and with the same gathering of condensation marks, it can be an evidence of a DDOS attacks. In FDPM, the marks in different packets don't construct their size; no additional bandwidth is exhausted. In this work, we utilized IP header use, encoding plans .By utilizing this we can recognize attacks specified as of now. Intrusion Detection systems serves to distinguish attacks. In future, one can utilize distinctive strategies for detecting different sorts of attacks.

ACKNOWLEDGMENTS

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We are thankful to the authorities of Savitribai Phule Pune University, organized by IJARCSSE for their constant guidelines and support. We are also thankful to reviewer for their valuable suggestions. We also thank the college authorities for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

REFERENCES

[1] Y. Kim, “Remote sensing and control of an irrigation system using a distributed wireless sensor network,” *IEEE Trans. Instrum.Meas.*, vol. 57, no. 7, pp. 1379–1387, Jul. 2008.

[2] N. Nasser and Y. Chen, “Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network,” in *Proc. IEEE Int. Conf. Commun.*, Glasgow, Scotland, Jun. 24–28, 2007, pp. 1154–1159.

[3] M. Zapata and N. Asokan, “Securing *ad hoc* routing protocols,” in *Proc. ACM Workshop Wireless Secur.*, 2002, pp. 1–10.

[4] T. Baba and S. Mstsuda, “Tracing Network Attacks to Their Sources,” IEEE Internet Computing, vol. 6, no. 3, pp. 20-26, 2002.

[5] Y. Xiang, W. Zhou, and J. Rough, “Trace IP Packets by Flexible Deterministic Packet Marking (FDPM),” Proc. IEEE Int’l Workshop IP Operations and Management (IPOM ’04), pp. 246-252, 2004.

[6] L. Buttyan and J. P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.

[7] T. Anantvalee and J. Wu, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks,” in *Wireless/Mobile Security*. New York: Springer- Verlag, 2008.

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehaviour in mobile ad hoc networks,” in *Proc. 6th Annu. Int. Conf. Mobile Comput. Netw.*, Boston, MA, 2000, pp. 255–265.

[9] J.-S. Lee, “A Petri net design of command filters for semiautonomous mobile sensor networks,” *IEEE Trans. Ind. Electron.*, vol. 55, no. 4, pp. 1835–1841, Apr. 2008.

[10] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, “Video transmission enhancement in presence ofmisbehaving nodes inMANETs,” *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, Oct. 2009.

[11] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, “An acknowledgment-based approach for the detection of routing misbehavior in MANETs,” *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.

[12] D. Johnson and D. Maltz, “Dynamic Source Routing in *ad hoc* wireless networks,” in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5, pp. 153–181.

[13] Botan, A Friendly C ++ Crypto Library. [Online]. Available: http:// botan.randombit.net/.

[14] TIK WSN Research Group, The Sensor Network Museum—Tmote Sky. [Online]. Available: http://www.snm.ethz.ch/Projects/TmoteSky.