International Journal of Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-2)

Research Article | **February 2015**

Intrusion Detection System Using EAACK on Man in the Middle, Replay and IP Spoofing Attacks

Aditi. R. Sangoram*, Yugandhara. A. Konde, (Asst. Prof.) **Rohini. G. Pise**
Department of Information Technology, Pimpri Chinchwad College of Engineering,
Pune, Maharashtra, India

Abstract—

The movement to wireless system from wired system has been a worldwide pattern in the recent decades. Among all the wireless systems, Mobile Ad hoc Network (MANET) is a standout amongst the most critical and special applications. Nodes correspond specifically with one another when they are both inside the same correspondence range. Else, they depend on their neighbours to transfer messages. The planning toward oneself capacity of nodes in MANET made it prominent among critical mission applications like military utilization or crisis recovery. In this paper, we proposed intrusion detection framework named Enhanced Adaptive Acknowledgment (EAACK) extraordinarily intended for MANETs. We have used three techniques, namely, IP header utilization, encoding schemes and replay detection. We detect and analyse three types of attack. Man-in-Middle attack, IP snooping attack and replay attack. It helps for intrusion detection. Analysed to contemporary methodologies, EAACK exhibits higher malicious detection rates in specific circumstances while does not incredibly influence the system performance.

Keywords— Enhanced Adaptive Acknowledgment (EAACK), Mobile Ad hoc Network (MANET), Intrusion Detection System (IDS), Man in Middle attack (MIM).

I. INTRODUCTION

Wireless networks are preferred till its invention because of their scalability and mobility. Owing to the enhanced technology and decreased costs, remote systems have increased significantly more inclination over wired systems in the recent decades. By definition, Mobile Ad hoc Network (MANET) is a gathering of versatile nodes furnished with both a wireless transmitter and a recipient that correspond with one another through bidirectional remote connections either straightforwardly or by implication. Modern remote access to and control by means of remote systems are getting to be more mainstream nowadays [1]. One of the real points of interest of wireless systems is its capacity to permit information correspondence between diverse gatherings and still keep up their mobility. Nonetheless, this correspondence is restricted to the scope of transmitters. This implies that two nodes can't correspond with one another when the separation between the two nodes is past the correspondence scope they could call their own. MANET tackles this issue by permitting intermediate parties to relay information transmissions. This is accomplished by isolating MANET into two sorts of systems, to be specific, single-hop and multihop.

In a single hop organize, all nodes inside the same radio extent communicate specifically with one another. On the other hand, in a multihop system, nodes depend on other transitional nodes to transmit if the end of the destination node is out of their radio range. MANET is equipped for making a configuring toward oneself and maintaining toward oneself up system without the assistance of an unified infrastructure, which is regularly infeasible in discriminating mission applications like military clash or crisis recovery. Insignificant design and fast development make MANET prepared to be utilized as a part of circumstances in emergency where a framework is occupied or unfeasible to introduce in situations like characteristic or human-instigated disaster, military clashes, also therapeutic emergency circumstances [2], [3]. Owing to these special attributes, MANET is getting to be more broadly executed in the business [4], [5]. Then again, considering the way that MANET is famous among discriminating mission applications, system security is of basic criticalness. The open medium and remote appropriation of MANET make it powerless against different sorts of attacks. Case in point, because of the nodes absence of physical insurance, malicious attacker can undoubtedly catch and node capturing to attain to attacks. Specifically, considering the way that most directing conventions in MANET accept that each node in the system carries on helpfully with different nodes and probably not malicious [6], attackers can undoubtedly bargain MANET by embeddings malicious or no cooperative nodes into the system. Moreover, as a result of MANET's disseminated building design and evolving topology, a conventional centralized monitoring system is not feasible in MANET. In such case, it is pivotal to create an Intrusion Detection System (IDS) exceptionally intended for MANETs.

In the next section II we are focusing on related work. In section III we focuses on implementation work and finally ended with IV section in results.

II. RELATED WORK

Anantvalee and Wu [7] exhibited an exceptionally careful overview on contemporary Ids in MANETs. In this section, we for the most part three current approaches, to be specific, Watchdog [8], TWOACK [9], and Versatile Acknowledgment (AACK) [10].

1) Watchdog: Marti et al. [8] proposed a technique of Watchdog that intends to enhance the throughput of system with the vicinity of malicious nodes. Truth be told, the Watchdog plan is comprised of two sections, in particular, Watchdog and Pathrater. Watchdog serves as an ID for MANETs. It is mindful for recognizing malicious node mischievous activities in the system. Watchdog recognizes malicious mischievous activities by wantonly listening to its next hop's transmission. On the off chance that a Watchdog node catches that its next node neglects to forward the packet inside a certain period of time, it builds its counter of failure. At whatever point a node's counter of failure surpasses a predefined edge, the Watchdog node reports it as acting mischievously. For this situation, the Pathrater collaborates with the routing protocol to maintain a strategic distance from the reported node in future transmission.
2) TWOACK: As for the shortcomings of the Watchdog plan, numerous specialists proposed new methodologies to unravel these issues. TWOACK proposed by Liu et al. [11] is a standout amongst the most critical methodologies among them. On the in spite of numerous different plans, TWOACK is not one or the other neither an upgrade nor a watchdog-based plan. Meaning to purpose the collision of receiver and restricted transmission power issues of Watchdog, TWOACK distinguishes acting up connections by recognizing each information packet transmitted over every three continuous nodes along the way from the source to the objective. Upon recovery of a packet, every node along the course is needed to send back an acknowledgement of packet to the node that is two hops far from it down the course. TWOACK is needed to take a shot at routing protocol, for example, Dynamic Source Routing (DSR) [12].
3) AACK: Based on TWOACK, Sheltami et al. [10] proposed another plan called AACK. Like TWOACK, AACK is based on acknowledgement system layer plan which can be considered as a blend of a plan called TACK (indistinguishable to TWOACK) and an end-to-end plan for acknowledgement called Acknowledge (ACK). Contrasted with TWOACK, AACK altogether lessened system overhead while still equipped for keeping up or actually surpassing the same system throughput. Truth be told, a large portion of the current Ids in MANETs embrace an affirmation based plan, including TWOACK and AACK. The capacities of such detection plan all generally rely on upon the acknowledgement packets. Henceforth, it is urgent to ensure that the acknowledgement packets are authenticating as well as valid. To address this worry, we embrace a computerized mark in our proposed plan named Enhanced AACK (EAACK).

III. IMPLEMENTATION DETAILS

A. IP Header Utilization

FDPM is focused on Ipv4. Conceivable Ipv6 usage of FDPM will include including an extension header in Ipv6 packet, which is diverse with the Ipv4 design. The need of FDPM Ipv6 usage needs more research in light of the fact that Ipv6 has inherent security systems, for example, authentication headers to give origin verification.

Three fields in the IP header are utilized for checking; they are Type of Service (TOS), Fragment ID, and Reserved Flag. The TOS field is a 8-bit field that gives a sign of the dynamic parameters. The subtle elements of taking care of TOS and particular of TOS qualities can be found in [13]. Subsequently, in FDPM, the TOS field will be utilized to store the mark if the network system convention does not utilize the TOS documented.

Section ID and Reserved Flag are additionally exploited. Given that under 0.25 percent of all Internet activity are fragment [14], Fragment ID can be securely over-loaded without bringing about genuine similarity issues.

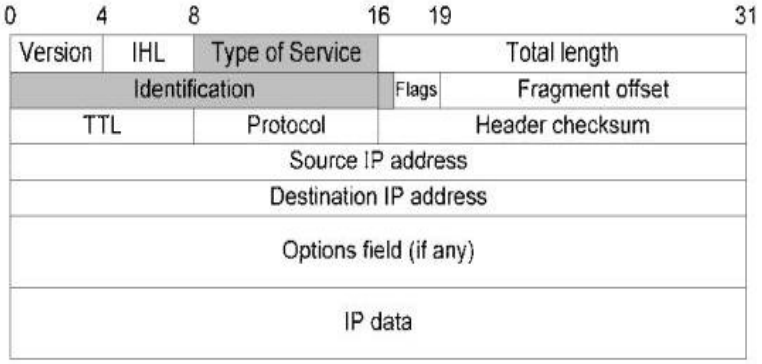

Fig. 1 The IP header fields in FDPM

B. Encoding Scheme

Before the FDPM mark can be created, the length of the mark must be resolved focused around the network system conventions deploy inside the system to be ensured. As per distinctive circumstances, the mark length could be 24 bits in length at most, 19 bits at centre, and 16 bits in any event. Hence, the adaptable length of the marks brings about three varieties of the encoding plan, which are named as FDPM-24, FDPM-19, what's more FDPM-16 in whatever is left of this paper. FDPM encoding plan is indicated in Fig. 2. The entrance IP location is partitioned into k fragments and put away into packet named k IP. The padding scheme is used to partition the source IP address equally into k parts.

The segment number is utilized to structure the location bits into a right way. The address summary empowers the remaking procedure to perceive that the clusters being examined are from the same source. Without this part, the remaking procedure can't recognize packets originating from diverse sources, along these lines won't have the capacity to follow various IP packets.

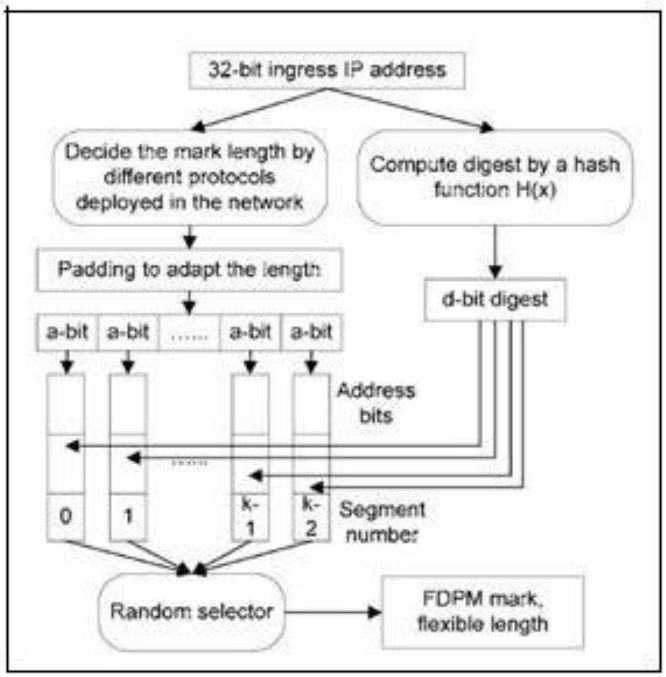

Fig. 2 FDPM encoding scheme

The encoding algorithm is demonstrated in Fig. 3. In FDPM, prior to the encoding procedure starts, the length of the mark must be computed. In the event that the TOS field in the IP packet is not utilized by the protected system, the 1-bit Reserved Flag in the header is situated to 0, and the length of mark is situated to 24. Under different circumstances, the length of mark will be 19 or 16, with bit(s) in TOS marked which are relevant. In the event that the system helps TOS Precedence however not TOS Priority, fourth to sixth bits of TOS are used for marking; and if the system helps TOS Priority however not TOS Precedence, first to third bits of TOS are used for marking.

```
1.  Marking process at router R, edge interface A, in network N
2.  Set the bit array Digest and Mark to 0
3.  if N does not utilize TOS
4.     Reserved_Flag:=0
5.     7th and 8th bit of TOS:=0
6.     Length_of_Mark:=24
7.  else
8.     Reserved_Flag :=1
9.     if N utilizes Differentiated Services Field or
10.    N supports Precedence and Priority
11.       7th and 8th bit of TOS:=1
12.       Length_of_Mark:=16
13.    else if N supports Precedence but not Priority
14.       7th bit of TOS:=1
15.       8th bit of TOS:=0
16.       Length_of_Mark:=19
17.    else if N support Priority but not Precedence
18.       7th bit of TOS:=0
19.       8th bit of TOS:=1
20.       Length_of_Mark:=19
21. Decide the lengths of each part in the mark
22. Digest:=Hash(A)
23. for i=0 to k-1
24.    Mark[i].Digest:=Digest
25.    Mark[i].Segment_number:=i
26.    Mark[i].Address_bit:=A[i[
27. for each incoming packet p passing the encoding router
28.    j:=random integer from 0 to k-1
29.    write Mark[j] into p.Mark
```

Fig. 3 Algorithm of FDPM encoding scheme

C. Replay Detection

The following algorithm is used for finding replay detection attack.

Replay detection algorithm:

For(Each packet)


```
{
        applyHash (packet)
        {
         For(i=0;I <4;i++){
        String Value =Apply _SHA(packet);
        }
}
      If(Filter created)
      {

        If(StringValue is present)
        {
            Replay Packet is detectd .
        }
       Else {
                    Filter_Add(packet);
            }
  If(replay packet detectd )
      {
        Find real replay attacker;
       }

}
```

IV. RESULTS AND DISCUSSION

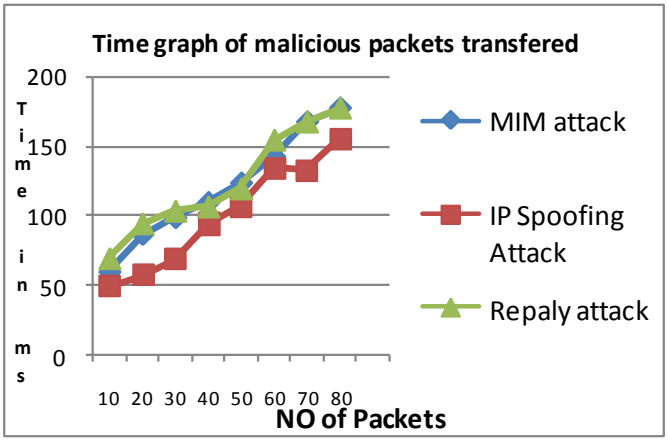

Fig. 4 Time Graph

The above figure 4 is graph for time. This is the time graph for the system which shows the transmission time for transmitting the number of packets in the presence of type of attack. In this graph on X-axis we show number of packets and time required for transmission of packets. Here replay packet require more time as it transmits the duplicate packets in this type of attack.

Table. 1 Transmission Time comparison between various attacks

	MIM attack	IP Spoofing Attack	Reply attack
10	60	50	70
20	87	58	95
30	99	69	104
40	110	95	107
50	124	108	120
60	143	135	155
70	168	133	168
80	178	156	178

In figure 5 depicts packet delivery ratio graph. This graphs shows that the malicious node vs packet delivery ratio for all the three type of attack as the graph shows that the more malicious nodes present in the graph less the packet delivery ratio. Packet delivery ratio depends on the number of successfully packet delivered to destination.

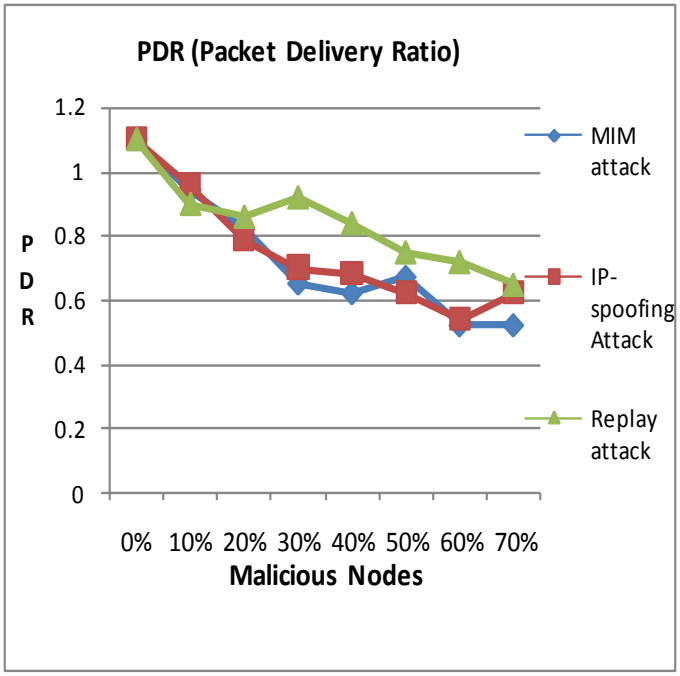

Fig. 5 Packet Delivery Ratio

V. CONCLUSION

FDPM is suitable for not just following sources of DDOS attacks additionally DDOS recognition. The primary normal for DDOS is to utilize various attacking sources to attacks a victimized person. Accordingly, at any point in the system, if there is a sudden surge in the various packets with the same destination and with the same gathering of condensation marks, it can be an indication of a DDOS attack. In FDPM, the marks in various packets don't build their size; no extra bandwidth is expended. Also with the over-burden avoidance capacity, FDPM can keep up the traceback process when the switch is vigorously stacked, though most present traceback plans don't have this over-burden anticipation ability. In this work, we used IP header utilization, encoding schemes and replay detection. By using this we can detect attacks mentioned already. Intrusion Detection schema helps to detect attack. In future, one can use different techniques for detecting various types 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 and concern members of conference, organized by IJERMT 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.

