IJMTARC – VOLUME – V – ISSUE - 17 – MAR 2017 ISSN: 2320-1363

A SECURED MECHANISM TO PREVENT THE VULNERABLITIES ON DDOS ATTACK TOWARDS WIRELESS NETWORKS

V.Santhosh[1], A.Sudhakar[2]

[1]Student, Department of CSE, Bharadhidasan Engineering College, Natrampalli, Tamilnadu, India

[2]Assistant Professor, Department of CSE, Bharadhidasan Engineering College, Natrampalli, Tamilnadu, India

Abstract

The Distributed Denial-of-Service (DDoS) attack is a serious threat to the legitimate use of the Internet. Prevention mechanisms are thwarted by the ability of attackers to forge or spoof the source addresses in IP packets. By employing Flooding, attackers can evade detection and put a substantial burden on the destination network for policing attack packets. In this project, we propose an inter domain packet filter (IDPF) architecture that can mitigate the level of Flooding on the Internet. A key feature of our scheme is that it does not require global routing information. IDPFs are constructed from the information implicit in Border Gateway Protocol (BGP) route updates and are deployed in network border routers. We establish the conditions under which the IDPF framework correctly works in that, that it does not discard packets with valid source addresses. IDPFs can proactively limit the spoofing capability of attackers. In addition, they can help localize the origin of an attack packet to a small number of candidate networks. In order to completely understand the attack mechanism, we examine the TCP / IP protocol suite. In the current system there is no method in place to ensure that the packet is properly delivered to the destination. The concept of IDPF overcomes the end to end packet transfer and acknowledgement during the intrusion or any malfunctioned activities. Hence the conversations via IDPF ensure data reliability as the recipient acknowledges for each and every packet.

CHAPTER 1

Introduction

Mobile Ad hoc Networks (MANET) have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET. Even though, there exist several intrusion response techniques to mitigate such critical attacks, existing solutions, typically attempt to isolate malicious nodes based on

IJMTARC – VOLUME – V – ISSUE - 17 – MAR 2017 ISSN: 2320-1363

binary or naive fuzzy response decisions. However, binary responses may result in unexpected network partition, causing additional damages to the network infrastructure, and naive fuzzy responses could lead to uncertainty in countering routing attacks in MANET. A risk-aware response mechanism is implemented to systematically cope with the identified routing attacks. Criminals have long employed the tactic of masking their true identity, from disguises to aliases to caller-id blocking. It should come as no surprise then, that criminals who conduct their nefarious activities on networks and computers should employ such techniques. Flooding is one of the most common forms of on-line camouflage. In flooding, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by "Flooding" the address of that machine.

The concept of Flooding was initially discussed in academic circles in the 1980's. While known about for some time, it was primarily theoretical until Robert Morris, whose son wrote the first Internet Worm, discovered a security weakness in the TCP protocol known as sequence prediction. Stephen Bellovin discussed the problem in-depth in Security Problems in the TCP/IP Protocol Suite, a paper that addressed design problems with the TCP/IP protocol suite. Another infamous attack, Kevin Mitnick's Christmas Day crack of Tsutomu Shimomura's machine, employed the Flooding and TCP sequence prediction techniques. While the popularity of such cracks has decreased due to the demise of the services they exploited, Flooding can still be used and needs to be addressed by all security administrators.

CHAPTER 2

Literature Survey

2.1 MITIGATING ROUTING MISBEHAVIOR IN MOBILE AD HOC NETWORKS

Sergio Marti[1], T J Giuli[1], and Kevin Lai[1] have proposed a scheme named Watchdog that aims to improve the throughput of network with the presence of malicious nodes. In fact, the Watchdog scheme is consisted of two parts, namely, Watchdog and Pathrater. Watchdog serves as IDS for MANETs. It is responsible for detecting malicious node misbehaviors in the network. Watchdog detects malicious misbehaviors by promiscuously listening to its next hop's transmission. If a Watchdog node overhears that its next node fails to forward the packet within a certain period of time, it increases its

IJMTARC – VOLUME – V – ISSUE - 17 – MAR 2017 ISSN: 2320-1363

failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. In this case, the Pathrater cooperates with the routing protocols to avoid the reported nodes in future transmission.

Many following research studies and implementations have proved that the Watchdog scheme is efficient. Furthermore, compared to some other schemes, Watchdog is capable of detecting malicious nodes rather than links. These advantages have made the Watchdog scheme a popular choice in the field. Many MANET IDSs are either based on or developed as an improvement to the Watchdog scheme. The Watchdog scheme fails to detect malicious misbehaviors with the presence of the following:

2.2 A PETRI NET DESIGN OF COMMAND FILTERS FOR SEMIAUTONOMOUS MOBILE SENSOR NETWORKS

Instead of using a client-server architecture, distributed peer-to-peer (P2P) communication between mobile robots is applied. The advantages of P2P include increased scalability (capacity scales with popularity), robustness (no single point of failure), fault tolerance, resilience to attack, and better support and management in distributed cooperative environments. Moreover, from a passive point of view, a command filter is proposed to avoid improper control actions from being carried out as the robot receives the human commands. The human operator sends command requests to the mobile robot through a wireless network. Inside the robotic computer, the command filter acquires the system status via distributed P2P communication and makes the decision to accept or reject the commands so as to meet the specifications, e.g., the collision avoidance among robots. The role of a command filter is to interact with the human operator and the mobile robot so that the closed human-in the-loop system satisfies the requirements and guarantees that undesirable executions never occur. PNs are used in designing the command filters, yielding a compact and graphical model for the MSN. Basically, the PN design of the filters is identical to the design of the supervisors in [10] and [11], except for the implementation framework. To demonstrate the feasibility of the proposed filtering framework, an application to a mobile wireless surveillance system is illustrated in this paper. During system operation, ensures that remote commands from the human operator meet the given collision avoidance requirements.

IJMTARC – VOLUME – V – ISSUE - 17 – MAR 2017 ISSN: 2320-1363

2.3 VIDEO TRANSMISSION ENHANCEMENT IN PRESENCE OF MISBEHAVING NODES IN MANETS

Assumptions and terminology

The bidirectional communication in every link between a pair of nodes. This means that, if a node N2 receives a packet from node N1, N1 can also receive a packet from N2. This is used to allow the acknowledgment to travel in the opposite direction. The misbehaving nodes that are just dropping the data packets while forwarding the control packets. These nodes also refuse to send acknowledgments to received data packets. Other types of misbehavior are not taken into account including colluding attack. The term AACK to refer to the combined scheme of TWOACK and end-to-end scheme. The two schemes that the system switches between them as TACK for TWOACK and AACK for end-to-end scheme.

Attack model

Adaptive acknowledgment scheme aims to detect the misbehaving node that intends to drop data packets whether this node is malicious or selfish node. These nodes cooperate with each other in the routing discovery phase to learn new routes. This cooperative environment involves both types of nodes, selfish nodes or malicious nodes that are engaged in path. The malicious nodes are classified into two types ordinary attackers and smart attackers. The main difference between the two types is that the smart attackers can do a receiver collision and limited transmission power

In a limited transmission power scenario the attacker adjusts its power transmission such that the signal strength is enough to be overheard by the sender. Upto 40% of the attackers as smart attackers and the rest as ordinary attackers that just dropping packets.

CHAPTER 3

SYSTEM REQUIREMENTS

HARDWARE CONFIGURATION

Processor	-	Pentium –IV
Speed	-	1.1 Ghz
RAM	-	256 MB(min)
Hard Disk	-	20 GB

SOFTWARE CONFIGURATION

Operating System	-	LINUX

IJMTARC – VOLUME – V – ISSUE - 17 – MAR 2017 ISSN: 2320-1363

Tool - Network Simulator-2

Front End - OTCL (Object Oriented Tool Command Language)

CHAPTER 4

Existing System

Packet-dropping attack has always been a major threat to the security in MANETs. A novel IDS named DDOS protocol specially designed for MANETs is proposed and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision.

DDOS

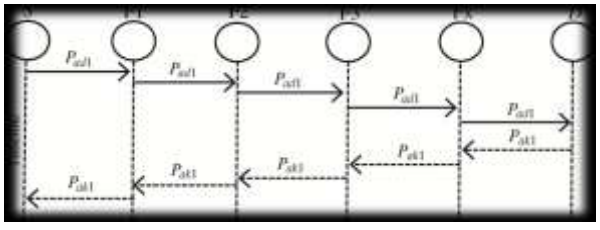

Figure 3.1 System control flow: This figure shows the system flow of how the proposed scheme works

DDOS is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). In order to distinguish different packet types in different schemes, we included a 2-b packet header in DDOS. According to the Internet draft of DSR, there is 6 b reserved in the DSR header. In DDOS, we use 2 b of the 6 b to flag different types of packets.

ACK

As discussed before, ACK is basically an end-to-end acknowledgment scheme. It acts as a part of the hybrid scheme in DDOS, aiming to reduce network overhead when no network misbehavior is detected. In Figure. 3.2, in ACK mode, node S first sends out an ACK data packet P_{ad1} to the destination node D. If all the intermediate nodes along the route between nodes S and D are cooperative and node D successfully receives P_{ad1}, node D is required to send back an ACK acknowledgment packet $P_{ak}i$ along the same route but in a reverse order. Within a predefined time period, if node S receives P_{ak1}, then the packet transmission from node S to node D is successful. Otherwise, node S will switch to S-ACK mode by sending out an S-ACK

IJMTARC – VOLUME – V – ISSUE - 17 – MAR 2017 ISSN: 2320-1363

data packet to detect the misbehaving nodes in the route.

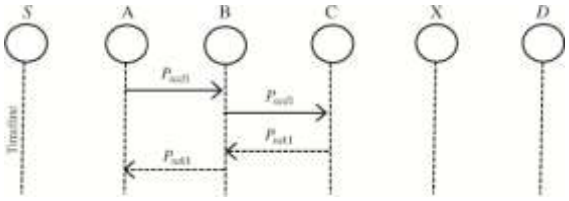

Figure 3.2 ACK scheme: The destination node is required to send back an acknowledgment packet to the source node when it receives a new packet

4.1 Disadvantages of Existing

DDOS scheme fails to detect malicious misbehaviors with the presence of the

following:

1) Ambiguous collisions
2) Collusion
3) Partial dropping

The TWOACK scheme successfully solves the receiver collision and limited transmission power problems posed by Watchdog. However, the acknowledgment process required in every packet transmission process added a significant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant transmission process can easily degrade the life span of the entire network.

The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead, but both TWOACK and AACK still suffer from the problem that they fail to detect malicious nodes with the presence of false misbehavior report and forged acknowledgment packets.

ARCHITECTURE

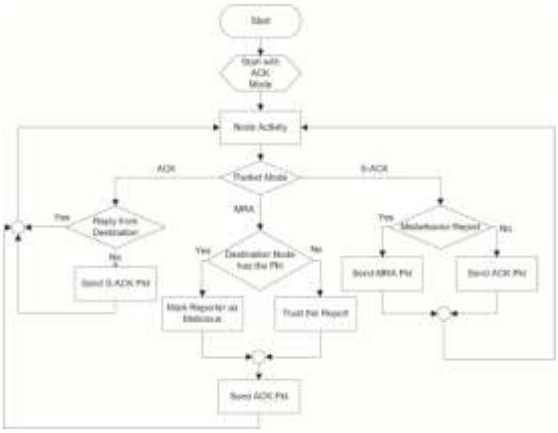

Figure 4.2 Architecture

CHAPTER 5

PROPOSED SYSTEM

The DDOS, methods to over efficient packet dropping in Mobile ad hoc network (MANET) is a self-organizing, self-configuring confederation of wireless systems. MANET devices join and leave the network asynchronously at will, and there are no

IJMTARC – VOLUME – V – ISSUE - 17 – MAR 2017 ISSN: 2320-1363

predefined clients or server. The dynamic topologies, mobile communications structure, decentralized control, and anonymity creates many challenges to the security of systems and network infrastructure in a MANET environment. Consequently, this extreme form of dynamic and distributed model requires a revaluation of conventional approaches to security enforcements. Associations between nodes are used to identify and isolate the malicious nodes. Simulation results show the effectiveness of our scheme compared with conventional scheme.

In MANET's each node may act as source or as a router. Nodes that cannot communicate directly depend on their neighbors in order to forward their messages to the appropriate destination. Applications of mobile ad hoc networks have increased requirements in order to ensure high quality of service for the provided services. Security in such infrastructure-less networks has been proven to be a challenging task. Many security threats arise against mobile ad hoc networks, as they are inherently vulnerable due to the way the build and preserve connectivity characteristics. The open medium presents the network with the first and most serious vulnerability. Unlike wired networks, ad hoc doesn't have any clear line of defense. Every node is vulnerable and the good performance of the network depends on every node or at least on every node participating in a path from the source to a given destination. So the security threats based on partial dropping, collusion, ambiguous collisions is given a solution in order provide a strong wireless MANET application.

5.1 ADVANTAGES OF PROPOSED

A node can circumvent the watchdog by dropping packets at a lower rate than the watchdog's configured minimum misbehavior threshold. Although the watchdog will not detect this node as misbehaving, this node is forced to forward at the threshold bandwidth. In this way the watchdog serves to enforce this minimum bandwidth. For the watchdog to work properly it must know where a packet should be in two hops.

IJMTARC – VOLUME – V – ISSUE - 17 – MAR 2017 ISSN: 2320-1363

CHAPTER 6

MODULES

6.1 Ambiguous collision

The ambiguous collision problem prevents A from overhearing transmissions from B. As Figure4.1 illustrates, a packet collision occur at A while it is listening for B to forward on a packet. A does not know if the collision was caused by forwarding on a packet as it should or if B never forwarded the packet and the collision was caused by other nodes in A's neighborhood. Because of this uncertainty, A should instead continue to watch B over a period of time.

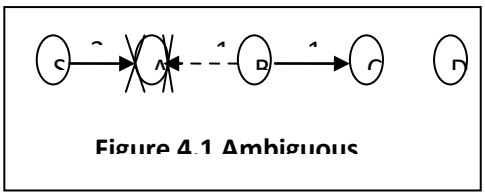

Figure 4.1 Ambiguous

Collusions

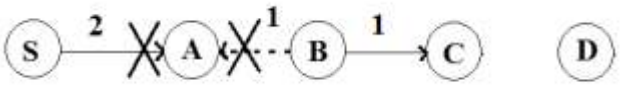

Figure 4.2 Collusion

- If two nodes in a row collude, the Watchdog mechanism is observed to be failed at that case, it is explained as follows,

  Node A sends a packet to colluding Node B.

  Node B forwards the packet to other colluding Node C.

  Node C drops the packet and Node B does not report it.

  Do not have two untrusted nodes in a row in a path.
- It assumes that the nodes act by themselves.

6.2 TECHNIQUES USED IN PROPOSED SYSTEM

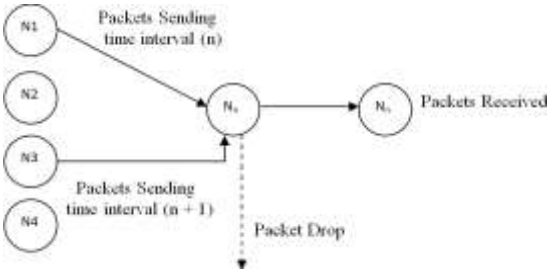

Figure 6.3 Structure Flow Diagram

A selective packet drop is a kind of denial of service where a malicious node attracts packets and drops them selectively

IJMTARC – VOLUME – V – ISSUE - 17 – MAR 2017 ISSN: 2320-1363

without forwarding them to the destination. As an example consider the scenario in figure 4.3. Here node 1 is the source node and node 7 is the destination node. Nodes 2 to 6 acts as the intermediate nodes. Node 5 acts as a malicious node. When source wishes to transmit data packet, it first sends out RREQ packets to the neighboring nodes. The malicious nodes being part of the network also receives the RREQ. The source node transmits data packets after receiving the RREP from the destination. As node 5 is also the part of routing path will receive the data packets and drops some of them while forwarding others. This type of attack is very hard to detect as the malicious nodes pretend to act like a good node.

The Association among the nodes and their neighboring nodes in to three types as below. In an adhoc network the Association between any node **x** and node **y** will be determined for the following defects.

6.3.1 Partial Dropping

In an adhoc network the Association between any node **x** and node **y** will be determined as follows.

Unknown

- Node x have never sent/received any messages to/from node y
- Trust levels between them are very low.
- Probability of malicious behavior is very high.
- Newly arrived nodes are grouped in to this category.

Known

- Node x have sent/received some messages to/from node y
- Trust levels between them are neither low nor too high.
- Probability of malicious behavior is to be observed.

Companion

- Node x have sent/received plenty of messages to/from node y
- Trust levels between them are very high.
- Probability of malicious behavior is very less.

The source selects the shortest and the next shortest path. Whenever a neighboring node is a companion, the message transfer is done immediately. This eliminates the overhead of invoking the trust estimator between companions. If it is a known or unknown, transfer is done based on the ratings. This protocol will converge to the DSR protocol if all the nodes in the ad hoc network are companions. Further the overheads due to

IJMTARC – VOLUME – V – ISSUE - 17 – MAR 2017 ISSN: 2320-1363

the calculations of trust relationship are minimal compared to the CONFIDANT protocol. It will be slightly more than the normal DSR due to the invocation of the trust estimator whenever a data transfer is to be done through known or unknown.

CHAPTER 7

Conclusion

Packet-dropping attack has always been a major threat to the security in MANETs. A novel IDS is specially designed for MANETs and compared it against other popular mechanisms in different scenarios through simulations. The results demonstrated positive performances against Watchdog, TWOACK, and AACK in the cases of receiver collision, limited transmission power, and false misbehaviour report. Further more, in an effort to prevent the attackers from initiating forged acknowledgment attacks, I extended our research to incorporate digital signature in our proposed scheme. Although it generates more ROs in some cases, as demonstrated in our experiment, it can vastly improve the network's PDR when the attackers are smart enough to forge acknowledgment packets. I think that this trade off is worthwhile when network security is the top priority.

In order to seek the optimal DSAs in MANETs, we implemented both DSA and RSA schemes in simulation. Eventually, we arrived to the conclusion that the DSA scheme is more suitable to be implemented in MANETs. To increase the merits of research work, to investigate the following issues in future research:

1) Possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature.

2) Examine the possibilities of adopting a key exchange mechanism to eliminate the requirement of pre distributed keys.

FUTURE WORK

In this approach we proposed a methodology to effectively filter the DDOS attacks and produced the scheme for prevention of attacks. The IDPF as specified above is a very effective countermeasure to the IP spoofing-based a flooding based DOS attacks. They rely completely on BGP update messages exchanged between neighboring nodes on the MANET to infer the validity of source address of a packet forwarded by a neighbor. However, it is demonstrated that the IDPFs

can be easily deployed on the current BGP-based Internet routing architecture. The simulation results also indicates that, even with partial deployment on the MANET, IDPFs can significantly limit the spoofing capability of attackers.

Moreover, they also help localize the actual origin of an attack packet to be within a small number of candidate networks.

In addition, IDPFs also provide adequate local incentives for network operators to deploy them. As future work, it is focused on the cost factor introduced by the filtering function on the forwarding path of packets and also planned to investigate how other AS relationship and routing information may help to further improve the performance of IDPFs.

REFERENCES

1. K. Al Agha, M.-H.Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B.Viollet, "Which wireless technology for industrial wireless sensor networks. The development of OCARI technol," *IEEE Trans. Ind. Electron.*,vol. 56, no. 10, pp. 4266–4278, Oct. 2009.
2. R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Network Security," in *Lecture Notes in Electrical Engineering*, vol. 127.New York: Springer-Verlag, 2012, pp. 659–666.
3. R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hocnetworks: A survey," in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana,India, 2012, pp. 535–541.
4. T. Anantvalee and J. Wu, "A Survey on Intrusion Detection in MobileAd Hoc Networks," in *Wireless/Mobile Security*. New York: Springer-Verlag, 2008.
5. L. Buttyan and J. P. Hubaux, *Security and Cooperation in WirelessNetworks*. Cambridge, U.K.: Cambridge Univ. Press, Aug. 2007.
6. D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, and L. Benini, "Modeling and optimization of a solar energy harvester system for self-powered wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 7,pp. 2759–2766, Jul. 2008.
7. V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks:Challenges, design principles, and technical

approach," *IEEE Trans. Ind.Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

8. Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl.*, 2002, pp. 3–13.
9. Y. Hu, A. Perrig, and D. Johnson, "ARIADNE: A secure on-demand routing protocol for ad hoc networks," in *Proc. 8th ACM Int. Conf. MobiCom*, Atlanta, GA, 2002, pp. 12–23.
10. G. Jayakumar and G. Gopinath, "*Ad hoc* mobile wireless networks routing protocol—A review," *J. Comput.Sci.*, vol. 3, no. 8, pp. 574–582,2007.
11. D. Johnson and D. Maltz, "Dynamic Source Routing in *ad hoc* wirelessnetworks," in *Mobile Computing*. Norwell, MA: Kluwer, 1996, ch. 5,pp. 153–181.
12. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting misbehaving nodesin MANETs," in *Proc. 12th Int. Conf. iiWAS*, Paris, France, Nov. 8–10,2010, pp. 216–222.
13. N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgementsin MANETs," in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis,Singapore, Mar. 22–25, 2011, pp. 488–494.
14. K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile *ad-hoc* communicationsin AEC industry," *J. Inf. Technol. Const.*, vol. 9, pp. 313–323,2004.
15. J.-S. Lee, "A Petri net design of command filters for semiautonomousmobile sensor networks," *IEEE Trans. Ind. Electron.*, vol. 55, no. 4,pp. 1835–1841, Apr. 2008.
16. K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "Anacknowledgment-based approach for the detection of routing misbehaviourin MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5,pp. 536–550, May 2007.
17. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviourin mobile ad hoc networks," in *Proc. 6th Annu.Int. Conf. MobileComput.Netw.*, Boston, MA, 2000, pp. 255–265.