International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 01 | Jan 2019 www.irjet.net p-ISSN: 2395-0072

A SURVEY:RESOLVING DISTRIBUTED DENIAL OF SERVICE ATTACK IN MANET

Ms. RASHMI P. BHURLEY[1], Ms. ARCHANA A. NIKOSE[2]

[1]M.Tech Student, Dept of CSE, PBCOE, Maharashtra, India
[2]Assistant Professor, Dept of CSE, PBCOE, Maharashtra, India

---

Abstract - *A Distributed Denial of Service flooding (DDoS) is biggest security concern it is overload the server, generate malicious traffic or interrupting the service. This issue crashes the host and the host service will be unavailable to the legitimate users. Although several defense systems have been proposed by researchers, the problem remains largely unresolved and unreliable for many attacks. In this paper, we present a mechanism that detects the misbehaving nodes. This approach is based on the two techniques which will be used in parallel in such a way that the results generated by one technique is further processed by the other to generate the list of misbehaving nodes. The first part detects the misbehaving link using the 2ACK technique and that information is used second part which uses AMD technique to detect misbehaving nodes.*

Key Words: *Distributed Denial of Service flooding attack, Mobile Ad hoc networks topology, nodes*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) can be used in a many applications from complex military operations to simple domestic environments. This makes security a important characteristic in WSNs. There have been various studies in the field of security in sensor networks, being Intrusion Detection System (IDS) is the most used tools among other tool in this area. This study proposes a new design based on reputation and trust of the different nodes of a network for decision making and search for possible source of malicious attacks.

1.1 Manet

Mobile Ad hoc networks (MANETs) are submissive to having their efficient operation compromised by a variety of security attacks because of the features like unreliability means which not to be trusted of wireless links between nodes, constantly changing topology, limited battery power, lack of centralized control and others. Nodes may misbehave either because they are malicious or it intentionally wishes to disrupt the network, or because they are selfish and wish to protect their own limited resources such as power. Each device in a MANET is free to move in any direction, and because of its nature it will change its links to other devices frequently. Important challenge in building a MANET is preparing each device to continuously maintain the information which is required to properly route traffic. This type of network may operate by them or may be connected to the larger Internet. It has different transceivers between nodes. There are some types of MANETs: closed and open. In a closed MANET, all mobile nodes help each other towards a common goal. In an open MANET, various mobile nodes with various goals share their resources in order to it happen global connectivity. An different mobile node may attempt to benefit from other nodes, but refuse to share its own resources, these nodes are called selfish nodes or misbehaving nodes and their behaviour is termed as selfishness or misbehaviour. Sources of energy consumption in the mobile nodes of MANETs are wireless transmission. A misbehaviour node may refuse to forward data packets for other nodes in order to conserve its own energy.

1.2 DDoS

A distributed denial of service (DDoS) attack is intended to cause damage to a computer system or steal private information from a computer system this attempt to make an online service unavailable to users, usually by temporarily suspending the services of its hosting server. This attack is different from other denial of service (DoS) attacks; it uses a single Internet-connected device (one network connection) for flooding a target with malicious traffic.

2. LITERATURE SURVEY

G. Acs, L. Buttyan, and L. Dora [1] in this paper, they of detect misbehaving routers in wireless mesh networks and then avoiding them while selecting the routes. They assume that link-state routing is used, and they propose a reputation system, where trusted gateway nodes compute Node Trust Values for the routers, which are fed back into the system and used for route selection procedure. The results show that there proposed mechanism can detect misbehaving routers reliably, it decrease the number of packets dropped due to router misbehavior considerably. At the same time, there mechanism only slightly increases the average route length. B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens [2] they discussed ad hoc networks offer increased coverage by using multihop communication. This architecture makes services influenced to internal attacks coming from compromised nodes that behave arbitrarily to disrupt the network, also referred to as Byzantine attacks. In this work, they examine the impact of several Byzantine attacks performed by individual or colluding attackers. They propose ODSBR, the first on-demand routing protocol for ad hoc wireless networks that provides resilience to Byzantine attacks caused by individual or colluding nodes. This paper demonstrates through simulations ODSBR's effectiveness in mitigating Byzantine attacks. It analysis the impact of these

attacks versus the adversary's effort gives insights into their relative strengths, their interaction, and their importance when designing multihop wireless routing protocols.

KeldorGerrigagoitia, RobertoUribeetxeberriay, UrkoZurutuzaz and lagnacio Arenaza[3] in this work they review the work done so far on Intrusion Detection Systems for WSN, they propose a new architecture based on the most suitable features of the reviewed systems that can lead to a complete and industrially usable IDS for WSN.In this work some IDS are proposed where special purpose nodes in the network which are important for monitoring other nodes. They listen to messages only in their same radio range and store message fields that can be useful to an IDS running in a sensor node. There are some other different points of view in the design of IDS in WSN, for example, where nodes are selfish and try to preserve their resources at expense of others. Other works keep the idea of no collaboration among sensor nodes and assume that the ad hoc network routing protocols can be applied to WSN.

H. Miranda and L. Rodrigues[4] an important characteristic of ad hoc networks is their self-organization, what makes them highly dependable of the participants. This paper shows how the selfishness of the participants in a ad hoc network can prejudice its overall functioning and sketches a protocol that discourages this kind of behavior. As previously mentioned, MANETs where visualize for search-and-rescue, military and law enforcement operations. In these examples, all users work together toward a common goal. Therefore, selfishness behavior is not expected since it would only prejudice the group. We envision that MANETs will rapidly expand to other domains, like the one presented above. In these Open MANETs, users do not share a common goal. Each user will agree to share their resources only if this brings them some benefit and not to the group as in Closed MANETs.

K. Liu, J. Deng, P. Varshney, and K. Balakrishnan [5] it describes the performance degradation caused by selfish (misbehaving) nodes in MANETs. They have proposed and evaluated a technique, to detect and mitigate the effect of such routing misbehavior.

W. Kozma Jr. and L Lazos[6]explains the problem of identification of misbehaving nodes and refusing to forward packets to a destination. They have proposed a reactive identification mechanism that does not rely on continuous overhearing or intensive acknowledgment techniques, but is only activated in the event of performance degradation.

S. Dhanalakshmi and, M. Rajaram [7] the work given in explains detection of malicious nodes by the destination node, isolation of malicious nodes by discarding the path and prevention data packets by using dispersion techniques.

D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C.-Y. Tseng, T. Bowen, K. Levitt, and J. Rowe [8] the work given in presents cooperative, distributed intrusion detection architecture for MANETs that is intended to address some challenges. This architecture is based on tree structure which has dynamic hierarchy in which acquisition of data occurs at the leaves, with intrusion detection data being aggregated incrementally, reduced, analyzed, and correlated as it flows upward towards the root.

3. CONCLUSION

In this paper, we present a mechanism that detect the misbehaving nodes and find the trusted and secure path to transfer the message from source to destination and we will resolve the ddos attack.

REFERENCES

[1] G. Acs, L. Buttyan, and L. Dora. Misbehaving router detection in link-state routing for wireless mesh network. In Proc. of WoWMoM, pages 1–6, 2010.

[2] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens. ODSBR: On demand secure byzantine resilient routing protocol for wireless ad hoc network. ACM Transactions on Information System Security, 10(4):11–35, 2008.

[3] Keldor Gerrigagoitia, Roberto Uribeetxeberriay,Urko Zurutuzaz and lagnacio Arenaza: Reputation based intrusion detection system for wireless sensor network.

[4] H. Miranda and L. Rodrigues, “Preventing Selfishness in Open Mobile Ad Hoc Networks,” Proc. Seventh CaberNet Radicals Workshop, 2002.

[5] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan. An acknowledgment based approach for the detecting of router misbehavior in Manets. IEEE Transactions on Mobile Computing, 6(5):536–550, 2007.

[6] W. Kozma Jr. and L. Lazos. REACT: Resource-efficient accountability for node misbehavior in ad hoc network based on random audit. In Proc. Of WiSec, 2009.

[7] S. Dhanalakshmi and, M. Rajaram, “A reliable and secure framework for detection and isolation of malicious nodes in MANET”, Int. J. Comp. Sci. Netw. Secur. vol. 8, no. 10, pp. 184–190,2008.

[8] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C.-Y. Tseng, T. Bowen, K. Levitt, and J. Rowe, “A general cooperative intrusion detection architecture for MANETs”, in Proc. 3rd IEEE Int. Inform. Assur. Worksh., College Park, USA, 2005, pp. 57–70.