DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.5144

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

SURVEY OF WATCHDOG MECHANISM USED FOR MALICIOUS NODE DETECTION

Mrs. C. Gayathri
Research scholar,
Department of Information Technology,
School of Computer Science and Engineering
Bharathiar University
Coimbatore TN - India

Dr.R. Vadivel
Assistant professor
Department of Information Technology
School of Computer Science and Engineering
Bharathiar University
Coimbatore TN- India

Abstract: A Mobile Ad-Hoc Networks is a type of wireless Ad-Hoc network and is self-configuring network of mobile routers linked by wireless links. It is a wireless network without infrastructure. Each device in MANET is free to move independently in any direction therefore change its links to other devices frequently. As an Ad-Hoc network which is deployed in such an environment which is physically insecure Intrusion Detection is one of the major areas of research is Ad-Hoc networks. This paper discusses on various Watchdog Techniques in MANET. Watchdog is a monitoring technique which detects the misbehaved nodes in the network. The main goal of in this paper focuses the various Watchdog Technique used for malicious node detection.

Keywords: *MANET, Attacks, Watchdog Mechanism.*

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are raising kind of wireless network technology, in which mobile nodes link on an extemporaneous or ad hoc basis. MANETs are self-forming and self-healing, enabling peer-level communications involving mobile nodes without reliance on centralized resources or fixed infrastructure. Mobile Ad-hoc network hosts are movable and flexible, and they communicate with each other within radio range, through direct wireless links, or multi hop routing. Due to its mobility and portability in wireless communication, it introduces data security threats, and security attacks.

The routing protocols in Mobile Ad-hoc networks are there to set up the most suitable path, between the source and destination, with minimum overhead and minimum bandwidth consumption. So that packets are delivered in a timely manner. In MANET routes are enabled in between the mobile hosts, using multi hop, as the transmission range of wireless radio is limited.

The hosts are responsible for passing through packets over Mobile Ad-hoc networks, and they are not aware of the topology of the network. Routing plays an important role in the security of the entire network. The mobility and portability in Mobile Ad-Hoc networks introduces security threats and security attacks. A change in topology means that security will have to be accessible, as nodes may be mobile, entering and leaving the network [1].

Mobile Ad-hoc networks routing protocols are exposed to various types of attacks, Black-hole attacks, being the most serious type. Fundamentally MANETs is self-forming, self-maintained, and self-healing, allowing for excessive network flexibility. MANET can be implemented as self-contained networks, or linked up to the internet, or private networks.

a. Characteristics of MANET

- In MANET, each and every node acts as together host and router. That is it is self-directed in activities.
- Multi-hop radio relaying- When a source node and destination node for a message is out of the communication range, the MANETs are able of multi-hop routing.
- Distributed character of operation for protection, routing and host configuration. A centralized firewall is not present here.
- The nodes can connection or leave the network anytime, making the network topology dynamic in nature.
- Mobile nodes are categorized with less memory, power and light weight features.
- The trustworthiness, effectiveness, permanence and capability of wireless links are often inferior when compared with wired links and this shows the changeable link bandwidth of the wireless links.
- Mobile and unstructured behaviour which demands minimum human intervention to arrange the network.
- Every node has equal quality with similar responsibilities and capabilities and hence it forms a totally symmetric background.

b. MANET Challenges

- A MANET environment has to overcome some issues of limitation and inefficiency. It includes:
- The wireless link uniqueness is time-varying in nature: There are communication impediments similar to fading, path loss, blockage and interference that add to the weak behavior of wireless channels. The dependability of wireless communication is resisted by different factors.
- Limited range of wireless transmission – The limited radio band outcome in reduced data rates compared to the wireless networks. For this reason optimal usage of bandwidth is essential by keeping low overhead as possible.
- Packet losses due to errors in transmission – MANETs familiarity higher packet loss due to factors such as hidden terminals that results in collisions, wireless

channel issues (high bit error rate (BER)), intrusion, and regular breakage in paths caused by mobility of nodes, increased collisions due to the being there of hidden terminals and bi-directional links.

- Route changes due to mobility- The dynamic nature of network topology results in standard path breaks.
- Regular network partitions- The casual movement of nodes often leads to division of the network. This naturally affects the in-between nodes.

c. Attacks in MANET

Dynamic topology, distributed operation, and resource constraints are some of the exceptional characteristics that exist in the ad hoc networks, which certainly increase the vulnerability of such network.
Many characteristics might be used to categorize attacks is passive vs. active and external vs. internal in the ad hoc networks.

Passive vs. active attacks

Passive attacks are launched to steal valuable information in the targeted networks. Examples of passive attacks in ad hoc network are eavesdropping attacks and traffic analysis attacks. Detecting this kind of attack is complicated because neither the system resources nor the critical network functions are physically affected to confirm the intrusions [2]. While passive attacks do not intend to disrupt the network operations, active attacks on the other hand actively alter the data with the purpose to obstruct the operation of the targeted networks. Examples of active attacks include actions such as message modifications, message replays, message fabrications and the denial of service attacks.

External vs. internal attacks

External attacks are attacks launched by adversaries who are not initially authorized to contribute in the network operations. These attacks typically aim to cause network congestion, denying access to specific network function or to disrupt the whole network operations. fake packets injection, denial of service, and impersonation are some of the attacks that are typically initiated by the external attackers.

II. RELATED WORKS

In Kachirski O et. al [3], the technique identifies misbehaving node by eavesdropping on the broadcast of the next hop. When a node forwards packets, Watchdog verifies whether the next node in the route forwards the packets or not. If the next node refuses to forward the packets, then it is identified as misbehavior. The advantages of Watchdog mechanisms that it can identify misbehaving nodes not in forwarding level but also in the level of connection. In other words, it identifies nodes not only in the link layer, but also in the network layer. Implementation of Watchdog is relatively easy. In this Watchdog has some obvious disadvantages. For example, due to the lack of cooperation in nodes, it may be unable to identify misbehaving nodes in circumstances such as 1) ambiguous collision 2) receiver collision 3) limited transmission power 4) false misbehaving 5) collision 6) minor dropping.

The watchdog technique [4] permits detecting misbehaving nodes. When a node forwards a packet, the watchdog set inside the node ensures that the next node in the path also forwards the packet. The watchdogs will this by listening to all nodes at intervals communication range promiscuously. If the node does not forward the packet, then it is considered as malicious node. A specific watchdog module is implemented and tested with the large number of nodes.

Kartik Kumar Srivastava [5], analyze the information switch over in a network of mobile and wireless nodes without some infrastructure maintain such networks are called as ad hoc networks. A Mobile ad hoc network (MANET) is mobile, multi-hop, infrastructure less wireless network which is accomplished of autonomous operation. In this paper discussed various of the basic routing protocols in MANET like Destination Sequenced Distance Vector(DSDV), Dynamic Source Routing(DSR), Ad-hoc On Demand Distance Vector(AODV) and Zone Routing Protocol(ZRP). Security is the main issue in MANETs as they are infrastructure-less and self-directed. Therefore, in manet networks with security requirements, there have to be two considerations kept in mind: one to make the routing protocol secure and second one to protect the data transmission. This method point out the achieving the routing and secure information exchange. This will make possible the user nodes to perform routing, mutual authentications, generation and secure exchange of session key.

III. METHODOLOGY

Watchdog Mechanism

Watchdogs are one of the best mechanisms to detect the threats and attacks from the misbehaved and selfish nodes in the networks. The Watchdog is used to improve throughput in a MANET, by identifying misbehaving nodes, which trick other nodes, by agreeing to forward the packets without ever doing so. While the watchdog is used to identify misbehaving (malicious) nodes, initiated by a Replica server, static method helps routing protocols avoid these nodes, by removing them, and creating a new path. The watchdog occurs in every node in the network.

Watchdog Mechanism in malicious node detection

There is various watchdog intrusion detection systems proposed to secure MANET. The watchdog IDS have advantage over other IDS is that they use only their local information and therefore they are robust to most of the attacks. Although importance of this mechanism is clear, it is hard to find studies that seriously test the watchdog in wireless mobile scenarios with high degree of mobility, characteristics of any Mobile Ad-hoc Network. There are different types of Watchdog Mechanism given below:

A. Collaborative Watchdog
B. Collaborative Watchdog with fuzzy logic
C. Improved Watchdog
D. Watchdog Based Clonal Selection Algorithm
E. Selective Watchdog Optimization Technique

A. Collaborative Watchdog

The Collaborative Watchdog Method reduce the overall detection time or selfish (or non collaborative) nodes in a network is the collaborative Watchdog [6]. This method worked with a log file in this mechanism. The collaborative

Watchdog Mechanism performs with selfish node at a particular time and saves the time. The Watchdog Mechanism follows neighbour node didn't forward the same data packets to its next hop node with in particular period it identified with misbehaving nodes.

The Collaborative Watchdog Method detects the selfish node in a correct way and reduces the false detection.

B. Collaborative Bayesian Watchdog with fuzzy logic

The Bayesian Watchdog method is a Fuzzy Logic Based Collaborative Watchdog approach. A Fuzzy Logic Based Collaborative Watchdog Mechanism is used to decrease the detection time of misbehaves nodes and increases the overall truthfulness [7]. This method increases the secure efficient routing by detecting the Black-Hole attacks.

Collaborative Bayesian Watchdog:

A Collaborative Bayesian Watchdog is based on message passing mechanism is every individual watchdog that allows publishing both self and neighbour reputations Bayesian Watchdog works suit for detects the Black-Hole attacks.

Fuzzy Logic:

Fuzzy Logic main concept is partial truth where the trust values range between completely true or false.

Process of Fuzzy Logic:

- Fuzzily all input values into fuzzy member function.
- Execute all applicable rules in the rule base to compute the fuzzy output function.
- De-fuzzifying the fuzzy output function to get crisp output values.
- A Collaborative Bayesian Watchdog method is increased the performance by decreased the amount of false negatives and speed up the detection process.

C. Hierarchical Design Based Improved Watchdog

The Improved Watchdog Technique basically based on Watchdog Mechanism is modified and improved by enhanced the security in Wireless Sensor Networks. The Improved Watchdog Technique also called as I-Watchdog [8]. This technique main concept is the Cluster Head monitoring the each and every cell of first layer of watchdog. If Node A wants to sends some data's to Node C, the Cluster Head performed that time as a Watchdog. The Cluster Head node uses a buffer which accommodates all the sent items by the nodes with in sensory limit. Node B is interface of the Node A and C. First Node A sends the data's to node B, after Node B received the message from A and compared with the message in the buffer. If the messages are same the first message in the buffer it will deleted.

Hierarchical Design

The Hierarchical model consumes the energy by the nodes in implemented with Intrusion Detection System in Wireless Sensor Networks. The Hierarchical architecture concept is the complete system divided into small parts. Each and every cell indicates the sensory limit of the Cluster Head node. The sensors system cells and topology are sometimes changeable. The only fixed nodes in the systems are the regional and Cluster Head nodes should be selected by the station at the outset of Network design.

D. Watchdog Based Clonal Selection Algorithm

The watchdog mechanism is defined to evaluate whether a node has abnormal behaviour in method of forwarding data. This Mechanism has a tendency to opt for Bio-Inspired Approach. In this paper, the Clonal selection principle is implemented and develop the Watchdog based Clonal Selection Algorithm (WCSA) [9].Using this WCSA, the intrusions in the network and monitoring multiple misbehaved nodes. This method follows hierarchical architecture. The complete network is divided into clusters. Each cluster indicates the sensory limit of a Cluster Head node. This algorithm can realize intruders and reduce the detector rate, and reduce generator value also will increase in throughput.

E. Selective Watchdog optimization Technique

The Selective Watchdog Optimization Technique is an improvement overcomes the Watchdog Technique. In Watchdog every node continually hears its next node transmission but the Selective Watchdog Method only when the acknowledgement would not be received then the IDS (Intrusion Detection System) is started.

Common Watchdog Technique all nodes monitor their neighbours but in this method the number of nodes divided into clusters and only nodes in the cluster which have greater value than threshold monitor their neighbours. This mechanism detects the intrusion in the presence of Black-Hole attack in the network and then routes the packets through secured path.

IV .CONCLUSION

Watchdog Mechanism is a fundamental building blocks to many trust systems that are designed for securing Mobile Ad-hoc Networks. Watchdog Technique is one of the Intrusion Detection Technique in ad-hoc networks. The above Watchdog Methods it represent with intrusion detection system being an important role of mobile ad hoc network. In this survey described the different types of Watchdog Mechanism involved the malicious node detection process. . It seems that the easier for the users to understand the Watchdog Mechanism.

REFFERENCES

[1] Anto Ramya S.I, "Mobile ad-hoc Netwoek Topology and its Algorithms", International Journal of Trend in Research and Development, Volume 2, No 5. Pp 16-21, Oct 2015.

[2] Narendra Reddy .P, Vishnuvardhan C.H, Ramesh.V, "Routing Attacks in Mobile ad-hoc Networks" Volume 2, No 5, pp 360-367, May 2013.

[3] O.Kachirski, R. Guha "Effective Intrusion Detection Using multiple sensors in Wireless ad-hoc Networks" International Conference on System Sciences, IEEE, 2003.

[4] S. Marti, T.J. Giuli, K. Lai, and M.Baker. Mitigating routing misbehavior in mobile ad hoc networks. 6th MobiCom, Boston, Massachusetts, August 2000.

[5] Karti kumar Srivasta, Avinash Tripathi, Anjnesh kumar Tiwari, "Secure Data Transmission in MANET Routing Protocol International Journal of Computer Technology& Applications, Volume 3, No 6, pp 1915-1921, Dec 2012.

[6] R. Bhuvaneshwari, G. Nalina keerthana, A. Rachel Roselin, "Improving Selfish Node Detection In MANET Using A Collaborative Watchdog" International Journal of Advanced Research Trends in Endineering and Technology, vol 3, No 15, pp 17-21, 2016.

[7] Harold Robinson, M. Rajaram, E. Golden Julie, S. Balaji, "Detection of Black Holes in MANET Using Collaborative Watchdog with Fuzzy Logic" International Journal of Computer and Information Engineering, Vol 10, No 3, pp 622-628, 2016.

[8] A. Forootaninia, M.B Ghazanvi-Ghoushchi " An Improved Watchdog Technique Based on Power-Aware Hierarchical Design for IDS in Wireless Sensor Networks" International Journal of Network Security & its Applications, Vol.4, No.4, 2012.

[9] S. Nishanthi "Intrusion Detection in Wireless Sensor Networks Using Watchdog Based Clonal Selection Algorithm" International Journal of Research in Engineering & Advanced Technology, Vol 1, No 1, 2013.

[10] Deepika dua and Atul Mishra "Selective Watchdog Technique for Intrusion Detection In Mobile Ad-Hoc Network" International Journal on Applications of Graph Theory in Wireless Ad hoc Networks and Sensors Networks, Vol.6, No.3, 2014.