IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Detect and Prevent the Occurrence of Selective Drop Attacks in WANET'S

N. REVATI[*1], S. KESAVARAO[*2]

[*1]M. Tech Scholar, Department of Computer Science & Engineering,

[*2]Assistant Professor, Department of Computer Science & Engineering,

Avanthi Institute of Engineering and Technology, (Affiliated to Jawaharlal Nehru Technological University, Kakinada) ,Cherukupally, Vizianagaram.

ABSTRACT

The process of sending packets from one location to another location under a dedicated shortest path is known as routing. There are several routing techniques in real world to send packets from one location to another location either in single path or multiple paths. One among the best is dynamic routing in which the data travel through multiple paths under dynamic manner. During the data transfer they may occur some attacks by the intruders who try to stop the packets not to reach the destination or sometimes they want to delay the packets transfer. In this current paper we try to investigate the problem of localizing node failures in communication networks from binary states (normal/ failed) of end-to-end paths. In this paper, we present a Resistive to Selective Drop Attack (RSDA) scheme to provide effective security against selective drop attack. If there is any attack occurred in the network, here we can able to provide an alternate path from the Point of Attack (POA) and can able to send the data packets in alternate best path. The network manager can able to find out the end to end path measurements on the network once the data transfer is completed. By conducting various experiments on our proposed model we finally came to a conclusion that our proposed approach is best in identifying the node failures in wireless adhoc networks (WANETs).

Key Words:

Resistive To Selective Drop Attack (RSDA), Dynamic Routing, Point Of Attack (POA), Node Failures, Wireless Adhoc Networks.

1. Introduction

In recent days security plays a very vital role in each and every organization like banking, software, shopping malls, E-commerce, Schools, Hospitals and so on. As security plays a very important role in real world environment but still a lot of users try to access the contents illegally and they want to misuse the content during transmission. In general there are several ways to create attacks on the packets which are sending from valid source to destination node. One form of attack is physical attack, where the attacker who tries to create attack will try to damage the content during the transmission from a selected source node to valid destination. Another form of attack is non-physical attack in which the data will not be physically damaged but the content will be delayed in service and it try to create some delay while transmission. One among the physical attack is forgery attack/packet modifier attack in which the intruder will select some nodes and intentionally try to drop those nodes and create attack on that specified node and make the data loss during communication [1].

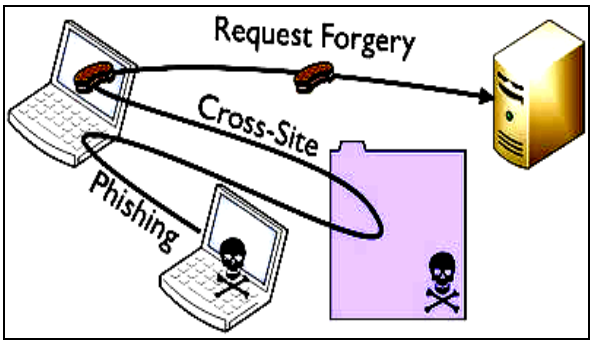

Figure 1. Sample Architecture of Selective Drop Attack

From the above figure 1,we can clearly identify that a sender node will try to browse the sensitive data and convert into packets before it is send to the destination node. The router will try to receive the data packets and choose best path among set of nodes which are present in the router window.During this data transfer, an intruder is the one who want to convert some nodes into abnormal state by stopping some nodes not to transfer the data to the destination nodes.These type of attacks are known as selective drop attacks.where the data which is to be send from a main node will be automatically converted into attack node and the data will be send in alternate path from the point of attack(POA) mode[2].Along with this selective drop attack there is also a chance of creating an attack like cross site and phishing in which they also comes under physical attack by damaging the content of end users. Generally a lot of criminals or intruders often target valuable sites like bank servers or credit card payment gateways or online shopping gateways and they try to make the process go with some modified values by changing the recipient account details or amount specified limit and then try to send those into their account, which in turn leads to attack [4],[5].

2. LITERATURE SURVEY

Literature survey is that the most vital step in software development process. Before developing the tool, it's necessary to work out the time factor, economy and company strength. Once this stuff is satisfied, ten next steps are to work out which OS and language used for developing the tool. This literature survey is mainly used for identifying the list of resources to construct this proposed application.

MOTIVATION

Two well-known authors Jiawei Li, and Athanasios [5], have written a paper on "Preventing Distributed Denial-of-Service Flooding Attacks with Dynamic Path Identifiers". In recent days almost all the network administrators try to find out the importance of path identifiers (*PIDs*) as inter- domain routing objects. These PIDs are almost static in nature and where the attacker try to create some sort of attacks within the network and they want to stop the packets not to be enter under the dedicated path,so this motived the authors to proposed dynamic PIDs in which the data can be send from valid source to destination under dynamic path and the data which is send from source to destination node are dynamic in nature and hence there will be an alternate path immediately if there is any attack found within the network.

Two well-known authors Issam Aib and Raouf Boutaba [6], have written a paper on "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks".In this paper the authors mainly discussed about the DDoS attacks which are exist in the distributed networks and how hard to find out those attacks in the network. In general these attacks are sometimes detected early and sometimes they become challenge to identify those attacks and take necessary step to protect the end users. The core nature of the proposed FireCol is composed of Intrusion Prevention Systems (IPSs) which is located in the ISP level. The evaluation of FireCol using extensive simulations and a real dataset is presented, showing FireCol effectiveness and low overhead, as well as its support for incremental deployment in real networks.

Two well-known authors James Joshi and David Tipper [7], have written a paper on "Defense Mechanisms against Distributed Denial of Service (DDoS) Flooding Attacks".In this paper the authors mainly discussed about the attacker who try to gain illegal access and try to attack the data. Once an attack army has been set up, an attacker can invoke a coordinated, large-scale attack against one or more targets. The process of designing a complete defense method against the DDOS Flooding attack is the desired goal for achieving the solution for the intrusion detection system and such a mechanisms require the complete understanding about the attacker and the influence of attacks over the network.

3. PROPOSED RESISTIVE TO SELECTIVE DROP ATTACK (RSDA) SCHEME

In this section we will mainly discuss about proposed approach for identifying the selective drop attacks which is created by the intruder within the network during data communication in a wireless sensor networks. Now let us discuss about this proposed model in detail as follows:

Motivation

The main motivation behind this detection of selective packet dropping attacks is to find out the packet drop attacks that were created by a malicious node inside the network. Initially we assume that links on the current path of our network exhibit the natural packet loss and there may be several adversary nodes that may present in the network during data transmission[8]. In general during the data transfer some nodes may become failed due to its internal functionality and some nodes may become attacked due to the external attacker who try to create attacks inside the network.For simplicity, we try to assume only linear data flow paths (i.e., as shown and described in Fig. 2a). Also, in this section we don't address the issue related to recovery of node once a malicious node is detected. All the Existing techniques that are available in the literature are almost orthogonal to our detection scheme and they may initiate multipath routing [9] when any compromised nodes occur within the network during the data transfer in one best path.

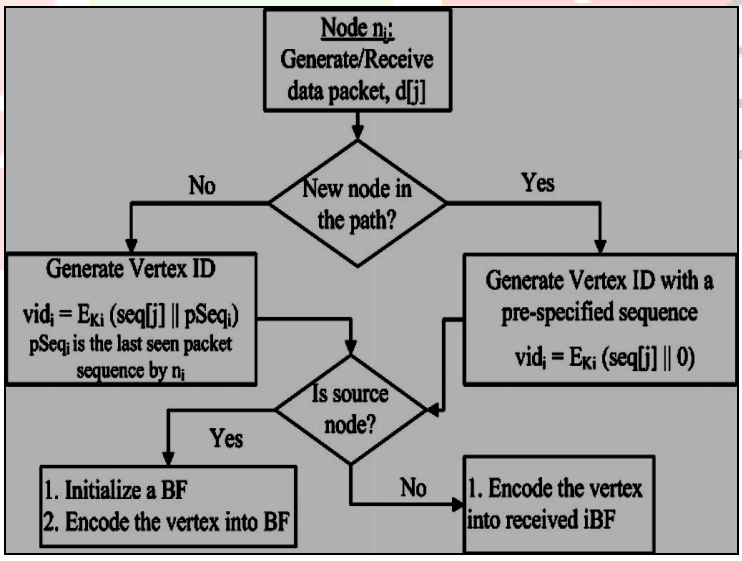

Figure 2 .Represents the proposed approach to Detect Packet Drop Attacks And Identify Malicious Nodes inside a WSN

Initially we try to prove the method of data provenance encoding for the packet acknowledgement that requires the sensors to transmit more meta-data. For each and every data packet ,a provenance record will be generated by a node and it will contains mainly of node ID and an ack for the node in the form of a unique sequence number of the last seen delivered or forward packet[10]. During the process of data transfer from one node to other node if there was any packets dropped due to intermediate nodes failure then we can

identify some nodes only can participate in sending the packets from valid source to destination and some are in active state of not carrying any data packets[11]. For this we consider a flow of data oath with term like "P" and n1 is nothing but the data source and we denote the link between the nodes n1 to ni as the li.

From the above figure, we can clearly find out the process of extended provenance encoding process. If we look at the figure in detail, each and every provenance record for a certain node includes the following fields like

1) The node ID,

2) An Acknowledgement of the last seen packet flow.

The Ack for the packets can be generated in several ways to serve this purpose. In our solution, a node ni creates a vertex vi for every jth packet it generates/forwards. The vertex ID$_{vidi}$ is generated as follows:

$$vid_i = generateVID(n_i, seq[j], pSeq_i) = E_{K_i}(seq[j] \| pSeq_i),$$

Where the fields like **pSeqi** is the knowledge of ni(i.e. Data provenance Update) about the sequence number of the previous packet in the flow.

ni is defined as the updates of the data provenance for the packet by inserting vidi into the iBF.

4. IMPLEMENTATION PHASE

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. The front end of the application takes Awt, Swings, Socket programming and as a Back-End Data base we took My SQL data base. The application is divided mainly into following 5 modules. They are as follows:

1. SOURCE MODULE

In this module, Source node will try to browse the file, select the destination and sends to the router. In Source while uploading the file, encrypt and then uploads the file. File content will be initialized to all the nodes. Here the source node chooses the text file for sending to the destination because the text files can only be converted into packets.

2. ROUTER MODULE

In this module, router consists of four Networks, each Network contains specific nodes. When Source sends the file initially it comes to the Network1 and passes through the Network1 nodes, if any congestion found in the Network1 node, It automatically selects the another node an moves to Network2 and Network 3 and Network4 and reaches the destination. The energy size also be modified, view the Network details. In router the routing path and time delay can be viewed.

3. ROUTER MANAGER MODULE

In this module, ROUTER MANAGER views the attacker details by checking the energy details and find attackers. This is used to provide an alternate path if there is any attack found during the data transmission.

4. DESTINATION MODULE

In this module, will receive the data from sender via router. The destination node can save the received data into its buffer location which is present in that application folder.

5. ATTACKER MODULE

In this module, attacker selects the Network and node, gets the original energy size and modifies the energy size for the node.

5. CONCLUSION

In this proposed paper we finally came to a conclusion that we proposed a new resistive to selective drop attack (RSDA) scheme which can able to provide an effective security for selective drop attack. It is important that the illegitimate nodes should be identified which overload a host and isolate them from the network by holding its transmission process. In the process of selective drop attacks all the nodes may not be loyal in sending the data from source to destination nodes, the neighboring nodes will not loyally forward their messages to the next node. Hence, our proposed application can able to identify such malicious nodes immediately and try to create an alternate path from the point of attack (POA) without disturbing the original path for transferring the specific messages.

6. REFERENCES

[1] Z. J. Haas, J. Deng, B. Liang, P. Papadimitratos, and S. Sajama, "Wireless ad hoc networks," *Encycl. Telecommun.*, 2002.

[2] S. Yousefi, M. S. Mousavi, and M. Fathy, "Vehicular ad hoc networks (VANETs): challenges and perspectives," in *ITS Telecommunications Proceedings, 2006 6th International Conference on*, 2006, pp. 761–766.

[3] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Commun. Mag.*, vol. 40, no. 10, pp. 70–75, 2002.

[4] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Comput. networks*, vol. 47, no. 4, pp. 445–487, 2005.

[5] V. Balakrishnan and V. Varadharajan, "Packet drop attack: A serious threat to operational mobile ad hoc networks," in *Proceedings of the International Conference on Networks and Communication Systems (NCS 2005), Krabi*, 2005, pp. 89–95.

[6] M. Peng, W. Shi, J.-P. Corriveau, R. Pazzi, and Y. Wang, "Black hole search in computer networks: State-of-the-art, challenges and future directions," *J. Parallel Distrib. Comput,2016.*

[7] J.-M. Chang, P.-C. Tsou, I. Woungang, H.-C. Chao, and C.-F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," *IEEE Syst. J.*, vol. 9, no. 1, pp. 65–75, 2015.

[8] A. Aijaz and A. H. Aghvami, "Cognitive Machine-to-Machine Communications for Internet-of-Things: A Protocol Stack Perspective," *IEEE Internet Things J.*, vol. 2, no. 2, pp. 103–112, 2015.

[9] P. Chen, S. Cheng, and K. Chen, "Information Fusion to Defend Intentional Attack in Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 337–348, 2014.

[10] X. Meng and T. Chen, "Event-driven communication for sampled-data control systems," *Am. Control Conf. (ACC), 2013*, no. 1, pp. 3002–3007, 2013.

[11] F. Razzak, "Spamming the Internet of Things: A possibility and its probable solution," *Procedia Comput. Sci.*, vol. 10, pp. 658–665, 2012.