Intrusion Detection Techniques for Secure Communication in Different Wireless Networks

Japneet Kaur, Harmeet Singh

Abstract—Technological advancement in the design of wireless communication have propelled an active interest in the field of Wireless Networks, Wireless Sensor Networks (WSNs), and Mobile Adhoc Networks (MANETs). Now days the speed and privacy are more reason of concern than the performance. The attacks can occur and there is always a chance that it will be a success. One of the major problems with Wireless Network security is that, all types of attacks are not known, and new ones emerge constantly [6]. Moreover, there is also a range of attacks that can be launched in the different mode, and thus making it more difficult for the Intrusion Detection System (IDS) to detect them. Therefore, main approach in network security is to detect and remove malicious intrusions. In this paper three different techniques have been proposed for securing Wireless LAN, WSNs and MANETs.

Keywords: Wireless Networks, Wireless LAN, WSNs, MANETs, Intrusion, IDS.

1. SECURING COMMUNICATION IN WIRELESS LAN

A mechanism for detecting and isolating session hijacking attacks is proposed which uses some rapid changes in the time taken between two nodes in the network[1]. The primitive function of the server is to discover the time passed when it recognizes RTS and CTS frame from the sender to recipient and vice versa [2].

For further reference, the time can be symbolized as,

$$TT = TT_M - TT_{s-r} - TT_{m-s} \qquad (1)$$

[22]

TT_{s-r} - To cover a distance between Sender & Receiver for the Ready to Send [3].

TT_{m-s} - To cover a distance between Server & Receiver for the Ready to Send [3].

TT_M - Time consumed for a $RTS-CTS$ handshake by the sender with the recipient.

The values of the Transmission Time at the server provide a reliable passive detection mechanism for the hijacking .The Transmission Time cannot be approximated as its value depends on[2]:

1) position of the receiver and the server
2) The distance between the server and receiver
3) The environment around the receiver and the server [3].

This is a property which cannot be measured or tricked by attacker when observing the network[7]. The time taken between two nodes an be tracked by passive server and any immediate changes are marked as suspicious [2].

The attacker can be identified who take over the receivers' session by tricking it and separating its MAC address [3]. On other side $RTS-CTS$ handshakes is used to identify the session hijacking attack which targets the sender. For example, dynamic RSS profile is built by the server and is updated continuously at every session and for every $RTS-CTS$ handshake, TT is calculated for MS2 as well as BS. If an attacker MS1 hijacks MS2 through spoofing its MAC address, the server will observe abrupt changes in the TT for MS2 and generates an alert signal. To detect the man-in-the-middle attacks against BS, The detection algorithm is as follows[8]:-

Detection Algorithm

Step 1: Server measures RSS

Step 2: Server measures TT

Step 3: Server calculates the weight W as

$$W = w1.\delta_{RSS} + w2.\delta_{TT} \qquad (2)$$

where δ_{RSS} = Variation of RSS and

δ_{TT} = Variation of TT

$w1$ and $w2$ are two constants, which can be fine tuned .

Step 4: If $W > Dthr$, (where $Dthr$ is the detection threshold) Then MS is an attacker.

By suitably adjusting the values of $Dthr$, and $w1$ and $w2$, we can reduce the false positive rate, significantly.

2. SECURING COMMUNICATION IN WIRELESS SENSOR NETWORKS

Based on the concept of Watchdog and Delphi, The Wormhole Resistant Hybrid Technique is developed. Hope counter value and gap-distance depends upon association of packet drop and RTT [1]. There is a possibility that normal route without Wormhole may turn out a high value of Round-trip time because of congestion in traffic and for

Revised Manuscript Received on July 18, 2019.

Japneet Kaur, MK Education Societies Group of Institutions, Amritsar.

Dr. Harmeet Singh, Assistant Professor, SBBS University, Jalandhar.

some other reason. On the other hand the affected route with Wormhole may results in little value of Round-trip-time due to longer distance. Furthermore, AODV is triggered due to less packet drop to pursue the path which is affected by wormhole path. Because of the above reason Wormhole exposure performance is negotiated when Delphi and Watch dogs comes into play in realistic WSN environments. Wormhole resistant hybrid techniques uses the data of packet drop and delay for the whole sensor network. The main motive is built the wormhole resistant hybrid technique that can handle all the categories of Wormhole without any major computation and cost [1]. It is an extension of AODV protocol. In AODV, time delay probability is calculated to find the existence of Wormhole in the path. Hope packet lose probability is computed in the next phase of Wormhole resistant hybrid technique. From the values of the Time Delay Probability and packet lose probability it can be found that the path include a Wormhole attack or not. In the proposed research Wormhole resistant hybrid technique locate the wormhole presence probability with the help of source node and a hope counter for a given path [1].

To find the occurrence of wormhole in a path time delay probability, time delay probability is computed for the AODV route discovery phase [1].

In the next phase of the WRHT, the probability per hop packet loss (PLP_H) is computed. It is used to compute the packet lose probability for the whole path. The values of time delay probability and packet lose probability are used for making the decision that the path contains a wormhole or not. The process of detection is initiated at time t_i by the sender for route request packet. The process of detection is initiated at time t_s by the receiver for route reply packet[1].

The round trip time can be specified as

$RTT_i = t_i - t_s$ then delay/hop value (DPH) of the path to the receiver via node i is given by

$$DPH_i = (RTT_i)/2h_i = (t_i - t_s)/2h_i. \quad (2)$$

Here h_i is the hop count field in the request reply of node i. for the calculation of per hope packet delay probability the difference between times and the mathematically it is defined as[4]

$$TDP_{HTOTAL}=TDP_{HRREQ} + TDP_{HRREP} \quad (3)$$

The time delay probability is a complete path can be defined as

$$(TDP_P) = 1 - (\prod_{j=1}^{n}(1 - TDP_j)) \quad (4)$$

Where, TDP_j is the time delay probability measured at node j.

The route discovery process will be ended if the value of the TDP_P is less than a predefined threshold (TH_{TDP}), if not then protocol fins the new route to the destination.

The process is shown in figure 1.

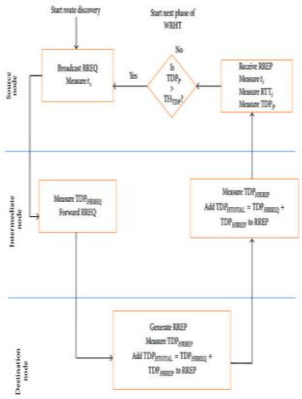

Figure 1: Route discovery process of WRHT

Fake Packets P_s is send on the defined route to investigate the presence of the wormholes. The recipient node receives the packet and in turn the destination node send back the acknowledgement of the number of the packets received[1].

The packet loss per path can be calculated through source node i by $PLP_i = P_s - P_r$. The per hop packet loss probability (PLP_H) can be computed by calculating the number of packets dropped at hop H to the number of packets received by hop H[1]. Mathematically, it is calculated as

$$1 - PLP_H \quad (5)$$

The packet loss probability of the complete path (PLP_P) is calculated as

$$(PLP_P) = 1 - (\prod_{j=1}^{n}(1 - PLP_j)) \quad (6)$$

Where, PLP_j is the packet loss probability measured at node j.

Figure 2 shows the process of PLP_P . the router is free from wormhole and is safe to use for communication If the value of PLP_P is less than a predefined threshold (TH_{PLP}). , if not, a new path will be found by sending are read request signal.

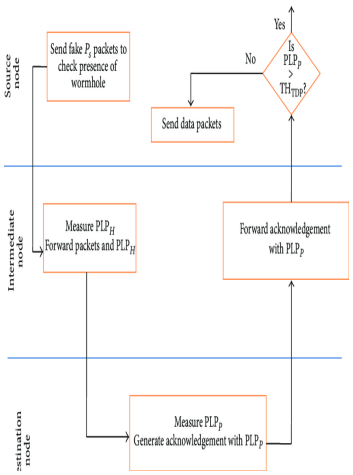

Figure 2: Wormhole detection process of WRHT.

3. SECURING COMMUNICATION IN MANET

For isolating selective packet drop attack in MANET, DHHP technique is proposed for improving the performance. The whole concept of detection and isolation depends upon two different techniques.

Diffie-Hellman algorithm is used for getting the secured path from source to destination [5]. HMAC technique for isolation of malicious nodes from the MANET.

In this mechanism, one node is selected from the insecure path in the direction of destination node. After selecting the particular node, the hash function is applied to the data packets at the source for obtaining MAC (Message Authentication Code) at the source node[4]. This MAC and data packet are transferred through an intermediate node which is part of the nodes in the insecure channel. Same hash function is applied at the destination node to the received data packet for obtaining new MAC. If MAC received from the source and MAC generated at the destination, both match with each other. It means path from source to destination through the particular node is secure, and then another node from the insecure channel will be selected as an intermediate node from source to destination. In another condition, if both MAC does not match at the destination node. It means path through the particular node is not secured and this node needs to be isolated from the network[5]. The malicious node which is selectively dropping the data packets is isolated from the MANET.

By using an HMAC based approach, the source node MAC is generated by encrypting messages with secret key using the Hash function. The original message and MAC are transferred collectively through the insecure channel and the performance of each of nodes in this channel is monitored by all of the monitoring nodes. At the destination node, again hash function is used to decrypt the data by using a secret key. The hash function is utilized to obtain the MAC from the message received by using the shared secret key. This MAC is compared with the MAC received along with the message at the destination. If both of these MACs do not match, it means the node through which data is obtained is selectively dropping the packets. The monitoring node will inform the central network administrator for isolating this malicious node from the network.

For the isolated node, the next best path is chosen from the stored paths by AODV protocol. This process of Diffie-Hellman is again repeated to get the secure path from source to destination node. If keys match at both of the ends, it means the path is secured and data will be transferred through that path. If keys do not match, it means there will be some malicious nodes which need to be isolated by using HMAC technique and the same process will be repeated to remove the malicious node and to establish a new secured path from source to destination. This process will be repeated until a secured channel is established from source to destination. In this way, the properties of both of the algorithms are utilized to improve the performance of MANETs under the AODV protocol. By using this hybrid technique, drawbacks of both existing techniques are also overcome.

4. SIMULATION RESULTS

The NS2 simulation tool is used on Fedora platform for the present research. The simulation results show that the proposed techniques attain low misdetection ratio [3]. The present investigation is also showing that there is false positive rate while increasing the packet delivery ratio.

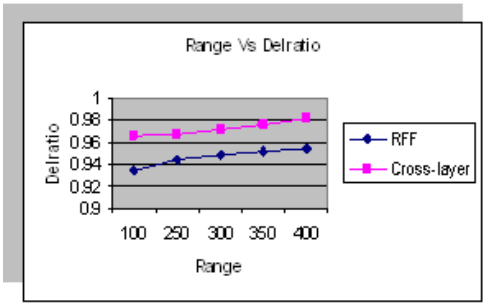

Figure 3: Range Vs Delivery Ratio

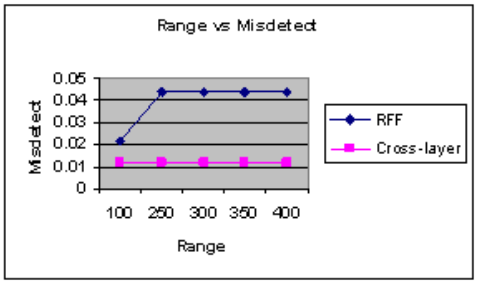

Figure 4: Range Vs Misdetection ratio

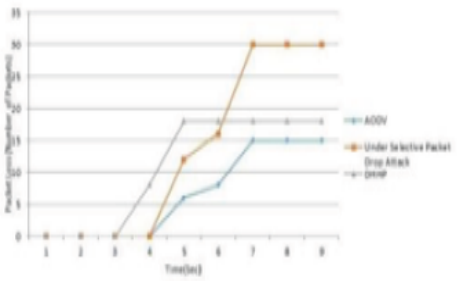

Figure 5: Decreased Packet Loss

5. CONCLUSION

In this paper, three techniques are proposed for secured communication in WLAN, WSNs, and MANETs. The first technique is a Cross Layer technique based on signal strength and time taken to protect WLANs from intrusions. The second technique proposed in this paper protect WSNs from Wormhole Attack. The technique is based on Watchdog and Delphi techniques. This hybrid technique secures sensor network in an efficient manner from wormhole attack by removing limitations of Watchdog and Delphi. The third technique proposed in this paper protects MANETs from Selective Packet Drop Attack. The Technique is based on Diffie-Hellman and HMAC function based techniques. The simulation results of all the proposed techniques in NS2 showed their efficiency against different parameters.

REFERENCES:

1. Rupinder Singh, Jatinder Singh, and Ravinder Singh published "WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks" I.K.G. Punjab Technical University, Kapurthala, Punjab, India Received 30 August 2016; Revised 23 October 2016; Accepted 2 November 2016
2. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.84.1595&rep=rep1&type=pdf
3. By George Coulouris, Jean Dollimore and Tim KindbergAddison-Wesley, ©Pearson Education 2001 Distributed Systems: Concepts and Design https://www.academia.edu/23740987/Chapter_1_Exercise_Solutions 2000
4. Rupinder Singh, Dr. Jatinder Singh & Dr. Ravinder Singh FUZZY BASED ADVANCED HYBRID INTRUSION DETECTION SYSTEM TO DETECT MALICIOUS NODES IN WIRELESS SENSOR NETWORKS" PUBLISHED IN 2016 HTTPS://WWW.SCRIBD.COM/DOCUMENT/357451353/3548607
5. Opinder Singh , Dr. Jatinder Singh & Dr. Ravinder Singh, DHHP: A Hybrid Technique for Protecting Mobile Adhoc Networks from Selective Packet Drop Attack International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 7 (2017), pp. 1743 -1763 © Research India Publications http://www.ripublication.com
6. Manish Kumar,Dr. M. Hanumanthappa, Dr. T. V. Suresh Kumar "Intrusion Detection Systems Challenges for Wireless Network" International Journal of Engineering Research and Applications (IJERA) ISSN: 22489622 www.ijera.com Vol. 2, Issue 1, Jan - Feb 2012, pp.274-280
7. [Kaur, Ravneet." Advances in Intrusion Detection System for WLAN" Advances in Internet of Things,2011
8. Opinder Singh,Jatinder Singh, Ravinder Singh, "An Intelligent Intrusion Detection and Prevention System for Safeguard Mobile Adhoc Networks against Malicious Nodes", Indian Journal of Science & Technology 2017