Indian Journal of Science and Technology, Vol 10(10), DOI: 10.17485/ijst/2017/v10i10/109291, March 2017
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Anomaly Prevention Mechanism for Wireless Networks using the Wireless Node Integrity Assessment Program

Rupinder Singh* and Dinesh Kumar

Department of Computer Science, Guru Kashi University, Sardulgarh Road, Talwandi Sabo, Bathinda – 151302, Punjab, India; dca.rupinder@gmail.com, kdinesh.gku@gmail.com

Abstract

Objectives: The wireless network security has been incorporated under this research, which has been implemented based upon the Secure Authentication Algorithm (SeAuL) for the wireless network security. **Methods/Statistical Analysis:** The multi-level authentication scheme has been proposed for the realization of the security among the wireless networks, which has been called Secure Authentication Algorithm (SeAuL). The proposed model has been designed in the pre-setup phase and post-setup phase for the robust authentication over the wireless networks. **Findings:** The proposed model has been equipped with the key based encryption using the 16-layered elliptic curve cryptography, which has been found more secure and rapid than the traditional AES algorithm in the various block sizes. The experimental results have proved the efficiency of the proposed model, when assessed on the basis of response delay for the encryption of the keys. **Application/ Improvements:** The anomaly prevention as well as the denial of service attack prevention has been implemented for the realization of the trusted wireless networks.

Keywords: Anomaly Prevention, Intrusion Avoidance, Intrusion Prevention, Secure Data Propagation, Wireless Network

1. Introduction

The IEEE 802.11 Wireless Local Area Network (WLAN) is expanded wireless technologies all over the world and feasible to play a major role in the next generation wireless communications networks[1]. The main attributes of 802.11 WLAN technologies are clarity, flexibility, portability and cost effectiveness[2]. This technology provides people with universal communications and enumerated environment in offices, hospitals, campuses, factories, airports, stock markets and so on. Synchronously, multimedia applications have experienced a hazardous growth[3-4]. People are now requiring receiving high speed audio, video, voice and Web services even when they are moving in offices or travelling around campuses. But, multimedia applications require some Quality of Service (QoS) support such as guaranteed bandwidth, delay, jitter and error rate[5]. Assuring those Quality of Service (QoS)[6] requirements in 802.11 WLAN is very challenging due to the QoS uninformed functions of its Medium Access Control (MAC) layer and the noisy and fluctuating PHY sical (PHY) layer characteristics[7].

The wireless Bandwidth estimation technique and the dynamic channel allocation model have been mostly based on the bandwidth required and the quality of service of IEEE 802.11e network[8]. The implementation technique was established in two different ways, one was centralized and another one was independent allocation. The results showed that the overall throughput bandwidth efficiency had been increased up to 30% without affecting in the individuals requirement of data transmission. The service rate of access point and bandwidth utilization becomes very important in the case of higher bandwidth data transfer over the WSN networks[9]. They discussed correlation among bandwidth utilization and

*Author for correspondence

capacity and focus on the effect of queue size on both of them. The results showed that:-

1. Capacity estimation exactly matches with queue size and inter arrived time.
2. Longer queue size introduced more collision in the network and results into significant reduction of capacity.
3. Higher packet generation rate by the STAs offers more collision for the AP.

The available bandwidth between two neighbor nodes and by extension along a path, to estimate each node's mediums occupancy including distant emissions, probabilistic of these values to account for synchronization between nodes, estimation of the collision probability between each couple of nodes, and variable overhead's impact estimation[10]. The result showed that single hop flows and multi hop flows were admitted more accurately resulting in a batter stability and overall performance. Results were encouraged in fixed networks as well as in mobile networks. **T**he MANET approach has been also studied for adjustment of the mobile Adhoc network, which was easy deployable LAN best suited for campus and office networks[11]. Therefore different types of data and file exchange are more than just normal message transmission. Hence a suitable mechanism was needed to provide this effectively. This study which was updated the technique incorporating the channel bandwidth as cost in the routing decision. We obtain multiple paths from source to destination and store the routes in a global route cache. The best path was reserved by audio traffic followed by video and data. We used Appropriate Traffic Generators for generating audio and video traffic from respective trace files. The MAC layer QOS mechanism made the 802.11e standard to support QOS in WLANs for real time applications[12]. The EDCA and HCCA survey mechanism was used. The HCCA applicable to infrastructure mode provided a deterministic QOS performance for applications with admission control. The EDCA was provided statistical QOS performance and used to both infrastructure and ad hoc mode.

2. Experimental Design

The proposed model is based upon the protection of the target wireless networks from the anomalies or vulnerabilities. The proposed model relies upon the authentication model to ensure the integrity of the nodes sending the data towards the destination node. The proposed model has been empowered with the model to mitigate the data overhead attacks over the wireless networks in order to control the anomalies as well as the resource engagement due to the heavy traffic caused by resource unavailability attacks. The flexible and robust authentication model along with the overhead filtering model has been utilized to overcome the attacks over the wireless network in the given scenario.

The pre-setup phase it utilized for the setup of the connection as well as the sharing of the key table among two nodes undergoing the wireless communication on the given channel during the given time. The whole procedure is elaborated in the following algorithm:

III.1 Pre-shared Key Generation Algorithm

1. Acquire the pre-shared information key
2. Compute the trigonometric equation in the standard set of keys in the given simulation:
$$S_{trigano} = Cos(S) * Sin(S) * log_{10}(S)$$
3. If $S_{trigano}$ produces the negative value convert this to the positive one by neutralizing the negativity factor using following simple mechanism:
$$S_{trigano} = -S_{trigano}$$
4. Produce the numeric key from the decimal key by shifting the decimal places to right by six places
$$S_{trigano} = S_{trigano} \times 10^{6}$$
5. Return the key value after rounding the key value to remove the decimal places
$$Key = round\,(S_{trigano})$$

III.2 Pre-setup Authentication Mechanism

1. When the wireless node (say X) receives the data from other source or it is intended to transmit the data towards the other node (say Y), which is not authentication yet, it begins the authentication procedure.
2. Node X triggers the authentication module, and queries the other end node to prepare and transmit the pre-shared information.
3. After completion of three-way handshake (TCP), the authentication procedure takes place following the pre-shared information request.
4. Node Y recalls the pre-shared information; process it using the algorithm III.1 transmit it back to node X.

5. Node X verifies the integrity of the pre-shared information key, and matches to the centralized database of nodes.
6. If data verification is successful

a. The Communication between node X and Y begins;
b. Otherwise, the communication channel between node X and Y ends and request terminated.

7. After the successful verification at step 6, then channel agreement bit is set to 1 to indicate the node integrity.

a. Each node X and Y sets their channel agreement bits to 1 for each other in the sparse table.

8. Generate and exchange the key table before establishing the communication over the given channel.

The key model has been explained in the detailed manner by taking the example of the two wireless nodes denoted X and Y in the given scenario. The authentication model has been leveraged to control the release and acceptance of the route information and other network topological data in order to protect the network from the external adversaries such as anomalies and denial of service attacks, which includes the three major types of attack, Distributed Denial of Service (DDoS), Denial of Service (DoS) and Selective Jamming. The key model utilizes the randomized key table generation, which is facilitated with the strong key generation algorithm

given with the $K_T = \sum_{n=1}^{k} f(v, x^1, x^2)$ for both of the sides in the wireless communication. In this equation the v denotes the seed value for the key table generation, whereas the x1 and x2 gives the number of rows and columns respectively.

Algorithm 1 : Secure Authentication Algorithm (SeAuL)

Step 1.Produce the key table with the given set details of row and column using the following equation:

$$K_T = \sum_{n=1}^{k} f(v, x^1, x^2)$$

Where KT is the key table, n denotes the initial value for the iteration counter and k gives the cap value for iteration counter. In the function f, the symbol v denotes the seed value for the key table generation, whereas the dimensions of the key table are taken in rows and columns and given by x1 and x2 respectively.

Step 2. Generate and assemble the key in the key table using the pseudo-random function based upon the permutation and combination mechanism with random weightage using the following equation under this key management algorithm.

$$Rk_i = fx(Kt_T Length)$$

Rk_i denotes the random indexfor iterative model

Step 3. The random key selection procedure takes places on the node sending or receiving the data, which is the practice of first step in the authentication mechanism across the wireless nodes. The key selection is based upon the random index generation in the limits of the key table size, which can be elaborated using the following equation:

$$\text{Key} = K_T(R_i, I)$$

$Where, R_i = pseudo - random\ index$ and I = Indicates the columns in the given table.

Step 4. Then the selected key is transmitted to the node on another end using the transmission socket, hereby given with the function fsocketx. The transmission socket requires the target information as well as the as the data for the transmission, which has been accomplished using the following equation:

$$fsocket_x(KeyData, NodeAddress)$$

Where KeyData represents the data, NodeAddress represents the information of the target node and fsocketx symbolizes the transmission socket.

Step 5. The other end node receives the data and returns the reply of the authentication key, which is produced by using the iterative mechanism to match the request or query key with the set of the query keys in order to determine the reply key. Then the reply key is formed out of the given table, which has been already shared among the wireless nodes during the pre-setup phase. The following equation is used for the key table lookup for the reply key in the given key table:

$$Key_A = \int^{n} [kt(nR, IC^2])$$

Where KeyA is the reply key produced on the other end using the kt lookup function, which requires the number of row denoted with nR and column series given by the symbol IC2.

Step 6. Then the first wireless node verifies the key information in order to produce the authentication decision:

If $K_A == K_T$, Authentication is successful, and denied otherwise.

3. Result Analysis

Blackhole Comparison: The defense against blackhole attack in the sensor network under the proposed model has been tested and compared with the existing blackhole detection and prevention model. The proposed model has been compared on the basis of average of delay and throughput. The proposed model comparison has been listed as below in table 1.

Table 1. The comparative analysis of the proposed model against existing model for blackhole attack

	Normal Flow	Under blackhole attack existing	Under blackhole attack proposed
End-to-End Delay (ms)	18.22	35.25	19.09
Throughput (bps)	170099.91	65072.06	143440

The proposed model has been found efficient in the terms of end-to-end delay and throughput. The proposed model is found at almost half the level of existing model on the basis of end-to-end delay, whereas approximately double at throughput. The comparative analysis proves the efficiency of the proposed model for detection and prevention of the black hole attack.

DDoS IDS Comparison: The distributed denial of service is also very hazardous attack like blackhole and contributes in the heavy data drop and resource usage due to the attack packets, which makes the performance of the attacker network weaker than the period of normal flow. The proposed model has been compared with the existing model for the detection and prevention of the DDoS attack over the sensor networks. The proposed and existing model comparison has been listed in table 2.

Table 2. The comparison between the existing and proposed model against the DDoS attack

The proposed model is found with less transmission delay than the existing model and lower number of dropped packets, which makes it efficient in comparison with the existing model. Also the proposed model is equally well in the case of total sent and received packets. The proposed model is also offering the data delivery percentage on approx. 96.65, which is again equal to the existing model. The proposed model can be proved better than the existing model on the basis of delay and lost packets.

4. Conclusion

The proposed model has been assessed against the existing model in order to mitigate the blackhole attacks as well as the DDoS attacks. The end-to-end delay in the normal flow of the traffic has been found nearly 18.22 in the wireless network. When studied the network under attack, the proposed model has been found with the 19.09, which is highly improved value than the 35.25 under the existing model in the attack scenario. Additionally the throughput of the traffic under the attack scenario has been tested at 143440 Kbytes for proposed model in comparison with the 65072 Kbytes for existing model, where the normal flow remains at the 170099 Kbytes in the wireless network. The proposed model clearly outperforms the existing model under the network with the blackholes. The pro-

Table 2. The comparison between the existing and proposed model against the DDoS attack

Performance Parameters	Normal Routing	Attack Case	IPS-Case existing	IPS-case proposed
SEND	2743	1159	2743	2743
RECV	2651	909	2651	2651
ROUTINGPKTS	1271	286828	1271	1271
PDF	96.65	78.43	96.65	96.65
NRL	0.48	315.54	0.48	0.40
Average Delay (ms)	615.66	586.34	615.66	21.4
No. of dropped data packets	87	250	87	50

posed model has been found effective and improved on the basis of the average delay and no. of dropped packets, as it has been studied on 21.4 ms and 50 packets respectively, which is highly improved in comparison of both of the techniques.

5. References

1. Senthil A and Logashanmugam E. Secure Acknowledgement based Misbehavior Detection in WSN (S-ACK). Indian Journal of Science and Technology. 2016 Oct; 9(40):1–6. Crossref
2. Fouad MMM and Hassanien AE. Key pre-distribution techniques for WSN security services. In Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations. Springer Berlin Heidelberg; 2014 jun. p. 265–83. Crossref
3. Kim MS, Park SK, Kim HS and Hwang K. An Efficient Key Management Scheme for Advanced Metering Infrastructure. In Advances in Computer Science and Ubiquitous Computing. Springer, Singapore; 2015 Dec. p. 125–30. Crossref
4. Biji N and Mala C. Analysis of ECC for application specific WSN security. In Computational Intelligence and Computing Research (ICCIC). 2015 Dec; p. 1–6.
5. Salehi S, Ahmad MA, Naraei RP and Farrokhtala A. Security in wireless sensor networks: Issues and challenges. In Space Science and Communication IconSpace; 2013. p. 356–60.
6. Said AA, Mantoro T and Tap AO. Improved Modified Reputation-Base Trust for Wireless Sensor Networks Security. Indian Journal of Science and Technology. 2016 Oct; 9(37):1–11.
7. Aznaoui H, Raghay S and Aziz L. New Smart nodes distribution using K means Approach to enhance Routing in WSN. Indian Journal of Science and Technology. 2016 Dec; 9(46):1–8. Crossref
8. Abdullah KM and Pervez AA. Wireless Bandwidth Estimation Technique (WBET) based dynamic channel allocation for IEEE802.11e standard. 2009 Oct; p. 294–99.
9. Arefin SK, Datta S and Das SK. A simplistic approach to model capacity estimation and bandwidth utilization of IEEE 802.11e WLAN. 2011; p. 1566–73.
10. Koujalrgi A. Bandwidth estimation for IEEE 802.11 based Ad Hoc Networks. International Journal of Thesis Projects and Dissertations (IJTPD). 2014; 2:1–25.
11. Sirgi S. A Routing protocol for efficient bandwidth utilization of IEE e in Ad-hoc network. International Journal of Engineering Research and Technology (IJERT). 2012 Sept; 1(7):1–5.
12. Acharya R, Vityanathan V and Chellaih PR. WLAN QoS issues and IEEE 802.11e QoS enhancement. International Journal of Computer Theory and Engineering. 2010 Feb; 2:143–49.