International Journal of Latest Trends in Engineering and Technology
Vol.(14)Issue(3), pp.026-030
DOI: http://dx.doi.org/10.21172/1.143.05
e-ISSN:2278-621X

MACHINE LEARNING FOR QOS OPTIMIZATION IN EARLY ATTACK DETECTION NETWORKS

Dharmaveer P. Choudhari[1], Sanjay. S. Dorle[2]

Abstract- Early attack detection in wireless networks generally requires a lot of computational steps, and pre-emptive calculations, which in turn reduce the quality of service (QoS) parameters like end to end delay of communication, the packet delivery ratio and most importantly the lifetime of the network. Such networks usually have high security performance, but compromise on crucial and time sensitive parameters, thereby making the networks inefficient for real time applications. In this paper, we propose a machine learning (ML) layer for optimization of the QoS parameters for early stage attack detection networks. The proposed protocol uses multiple one-time computational parameters which can be evaluated before network deployment, and then used recursively throughout the network's lifetime without much modifications. Evaluation of the proposed protocol was done on various network scenarios, which indicated a 9% performance improvement in terms of end-to-end communication delay, and more than 15% improvement in terms of network lifetime, while it also shows about3% improvement in network throughput and packet delivery ratio, which is due to a trade-off in the fitness function of the proposed machine learning algorithm, and can be fine tuned as per the application's requirements. These optimizations are achieved without compromising on the network's attack detection probability.

1. INTRODUCTION

Early attack detection in networks basically means to detect and mitigate attacks in wireless networks before they can happen, so that the network is always running in optimal conditions. This ensures that the network has high packet delivery ratio, minimal energy wastage and optimal throughput. In order to perform early attack detection, the following steps are usually followed,

Network formation with signature parameters: In this step, the network formation is done, and some identifiable parameters (also called as signature parameters) are setup. These parameters include, node's configurations (like initial energy), the energy model (includes transmission energy, reception energy, and other energy parameters), the packet transmission and reception rates for nodes, any specific node signatures which might be needed like preamble bit sequences, and other parameters. This step is very crucial due to the fact, that is separates the designed network uniquely from any other networks

Node communication sequences: Once the network is setup, then the node communication sequences are setup, this step makes sure that the overall network communication is controlled by a given set of patterns, and in case there is a pattern mismatch, then the issue can be tracked and attackers (if any) can be identified. Examples can be wireless sensor networks, where various sensor nodes are connected with the base station, but the sensor nodes communicate only at a given time or event, so that collision avoidance can be achieved. Such a scenario can be observed in any kind of wireless network, including adhoc and cognitive radio networks as well.

Periodic signature evaluation: Upon network setup and node communication, the next important step in early attack detection is to check the signatures of the network traffic periodically, in order to find out any kind of abnormality in the communication. Various classifiers are used for signature analysis, including but not limited to neural networks, support vector machines, random forests, and many others. This step is the most computationally expensive step, and does not allow the router's computational unit to perform anything else apart from this computation, this leads to a lot of delay in the network packets, and in some cases of high speed networks, this is the main reason for packet drops, from the network queue due to flooding. Thus, designers of this unit need to take into consideration various parameters while designing the unit, and also a lot of research goes into pattern optimizations and classifier optimization.

Apart from these steps, some network designers follow application specific steps, like for military networks, nodes are concealed in protective cases, and the case signatures are used for identification. Due to these steps, the network's QoS parameters like end to end delay, throughput, energy consumption and packet delivery ratio takes a hit, and therefore there is a need to optimize these parameters along with early attack detection in the networks. Due to this fact, there is a need for an algorithm which works in tandem with the early attack detection algorithm, and allows for a better QoS for the network. In this paper, we propose a machine learning layer, which works in synchronization with the early attack detection algorithm namely distribution adaptive distance with channel quality (DADCQ). This machine learning layer ensures that the early attack detection technique does not deter the QoS of the system, with the help of the following machine learning steps,

It selects the most optimal routing path between a given source and destination

[1,2] Department of Electronics Engineering, G.H.Raisoni College of Engineering, Nagpur,MS,India

It selects the most optimal medium access protocol to be applied in the network
Due to these 2 properties of the machine learning algorithm, the network's QoS improves, and thus even after all the computational complexities which are presented by the early attack detection algorithm, the proposed network has a QoS which is as close to optimal as possible. The next section describes various early attack detection techniques, followed by the proposed early attack detection with QoS optimizing machine learning layer, and later followed by the comparison of QoS parameters which are presented by standard protocols, and we finally conclude this text with some good observations about our work, and how it can be taken further.

2. PROPOSED ALGORITHM

We first define the early attack detection protocol based on the DADCQ technique, followed by the proposed machine learning layer. The proposed DADCQ protocol takes advantage of the multiple thresholds supported by the protocol in order to evaluate the attackers in the system. The proposed protocol can be elaborated using the following modules,
a. Removal of Eavesdropping Attacks
Eavesdropping attacks occurs when the data is transmitted by authorized user and it is been read or received by the unauthorized user. So for this the DADCQ proposes the concept of adding the trusted nodes in the network those are fixed at the fixed distance in the network and these nodes are arranged in such a way that they cover the entire network. So the proposed method says that whenever the communication takes place it should satisfy the following equation:

$$Ecn\ max > (Ecs , Ecr) \quad (1)$$

Where Ecn is the communication node via which the communication is taking place and is also called as hop node, Ecs is the communicating source node; Ecr is the communicating receiver node. Ecn must follow the given condition.

$$Ecn \in (Etrusted) \quad (2)$$

Where Etrusted is the set of trusted nodes placed in the network. During the communication cycle the energy content of the Entrusted nodes is changed stochastically due to the rapid charging and discharging cycles so the attacker is not able to replicate it very easily. Also the node distance should follow the given equation:

$$Dcsnr > Dcsn + Dcrn \quad (3)$$

$$Dcsn < Dcsr \quad (4)$$

$$Dcrn < Dcsr \quad (5)$$

In the equations above Dcsnr is the Euclidean distance between the sources to communication node to receiver, Dcsn is the distance between the sources to communication node, Dcrn is the distance between the receiver and the
selected node, Dcsr is the direct distance between source and destination. The equations 3, 4 & 5 make sure that follows 6

$$Pc \in (Ptrusted) \quad (6)$$

Where Pc is the position of the selected node and Ptrusted is the set of the trusted nodes which are placed by in the network. Due to an infinite number of possible combinations of energy variations and an infinite number of nodes placements there is almost insignificant probability of eves-dropping attack by any node.

2.1 Removal of DDoS Attacks

DDoS attacks occur when lots to nodes try to communicate with the single entity node in the network. In order to remove DDoS attacks DADCQ uses the pattern analysis technique. In this technique the node patterns are evaluated and the patterns being transmitted by the nodes are evaluated. This technique works in 2 level of threshold comparison in the first level of threshold comparison the number of packets communicated by the node per unit time are monitored and the following threshold is applied as

$$Pputn < 1.5 * \Sigma\ Pputi /N \quad (7)$$

Where Pput is the number of packets transmitted per unit time by node n is number of node being screened for DDoS. N is the total number of nodes in the network. The selected constant is 1.5 is fixed for healthy communication so number of nodes communicated at any time by a single node is at most 1.5 times the mean value of packets communicated by all nodes. The factor 1.5 is fixed after performing more than 1000 communications in the network and observing the ratio of the packets communicated by a node to the mean of packets communicated in the network for a total of 200 nodes in each communication. The nodes which do not satisfy the above constraints are being identified and are marked as level DDoS attackers they are not blocked from communication but DADCQ gives lesser priority to these nodes while the re-broadcasting of the packets. Nodes can regain the trust values by sending the lower than threshold packets in the consecutive communications. Post the level1 marking the nodes whose trust values are found to be satisfying equation are marked as DDoS nodes and are given the lowest DADCQ priority in the communication sequence

$$Tvn < \Sigma\ Tvi /2* N \quad (8)$$

Where Tvn is the trust value of the scanned node post level 1 screening and Tv is the trust value of all the nodes and N is the total number of node. The factor 2*N is considered as to be sure that the identified node has as trust value lower than at least half of the trust values of all scanned nodes which do not satisfy the level 1 constraints in the network.The factor 2*N is considered, so as to be sure, that the identified node has a trust value lower than at least half of the mean of the trust values of

all scanned nodes which do not satisfy level 1 constraints in the network. So initially each node has a fixed factor until 0.1, if the nodes do not follow the equation (8).Where Tvn is the trust value of the scanned node post level 1 screening, and Tvi is the trust value of all the nodes, N is the total number of nodes.Due to the dynamic nature of thresholds, it is very easy for the network designer to identify DDOS affected nodes, and make sure that they are not a part of the communication sequenceThe nodes which satisfy the constraints given by both the eves-dropping and DDOS techniques are further allowed to perform communication, while others are dropped from the communication sequence. Before application of the early attack detection algorithm on the network, the machine learning layer is applied for communication and medium access control in order to get optimum QoS.

3. EXPERIMENT AND RESULT

The network parameters used are defined as follows,

Parameter	Value
Routing algorithm	AODV
Number of nodes	30 to 100
Network type	P2P
Queue	Priority drop tail
Network size	300 m x 300 m
MAC Type	802.11
No.of communications	1-50
Protocols used	p-persistence, DCB, AAG, ML with DADCQ (proposed)

Table .1. Network parameters

Number of Communications	p-persistence Delay (ms)	DCB Delay (ms)	AAG Delay (ms)	Proposed Delay (ms)
5	2.36	2.38	2.32	1.86
10	2.75	2.36	2.33	1.96
20	2.96	2.77	2.35	2.13
40	3.18	2.89	2.37	2.22
80	3.31	2.93	2.38	2.27
100	3.48	2.97	2.42	2.33
150	3.63	3.01	2.53	2.41

Table.2. Comparison of Mean End To End Communication Delay

From table 2, we can observe the end to end communication delay post removal of attack for the proposed algorithm is at par with the standard techniques, and is further reduced with the help of the proposed machine learning layer. The next comparison was done for the energy consumption of the network during attacks. It is observed that the proposed algorithm not only keeps a similar energy profile when compared to the existing algorithms, but it also improves upon the energy consumption of the network, and thus can be used by network designers for designing real time networks,

Number of Communications	p-persistence Energy (mJ)	DCB Energy (mJ)	AAG Energy (mJ)	Proposed Energy (mJ)
5	5.79	5.99	4.89	4.39
10	6.37	7.23	6.56	5.31
20	8.96	8.36	8.25	6.73
40	12.58	14.33	13.48	10.63
80	15.32	15.52	15.02	12.07
100	17.39	18.13	17.79	14.03
150	19.91	20.75	20.51	16.10

Table.3. Energy comparison

As the proposed algorithm improves the lifetime of the network, and also improves the speed of communication even under DDOS and eves-dropping attacks, the network is bound to perform well in terms of packet delivery ratio and overall communication throughput. The following tables depict this nature of the algorithm,

No. of Comms.	PDR (%) with attack	PDR (%) Watchdog	PDR (%) Traceback	PDR (%) Proposed
5	98	98	99	99.61
10	99	99	97	99.45
15	97	99	99	99.54
20	98	99	99	99.66
25	97	98	97	99.55
30	97	99	99	99.84
35	99	99	99	99.88
40	98	99	97	99.58
45	97	99	99	99.66
50	99	99	97	99.77

Table.4. Comparison of PDR

Due to higher speed, the network is able to communicate a greater number of packets over a single time slot, thus the value of throughput improves. Moreover, due to the early attack detection there are no attacks in the network, therefore there is limited packet drops. This is observed from table 4, that the overall network packet delivery ratio improves due to the proposed attack removal technique with machine learning layer. Another parameter which indicates high QoS is the network throughput. A high value of throughput generally means that the network under consideration is capable of sending higher number of packets over the network and the receiver is able to receive them without drops. In Table 5 we can observe that the proposed protocol has better throughput as compared to the existing ones, and thus it improves on the QoS of the overall network.

Number of Communications	p-persistence Throughput (kbps)	DCB Throughput (kbps)	AAG Throughput (kbps)	Proposed Throughput (kbps)
5	215.80	237.38	226.59	242.78
10	217.60	221.95	219.78	235.47
20	229.30	243.06	236.18	253.05
40	238.10	259.53	248.81	266.59
80	246.73	273.87	260.30	278.89
100	249.31	269.25	259.28	277.80
150	251.66	276.83	264.24	283.12

Table.5. Comparison of Network Throughput

From the above results, we can observe that the overall network QoS is massively improved with the help of the proposed machine learning based early attack detection algorithm which uses DADCQ, and that the network performs better even in the presence of network attacks.

4. CONCLUSION

Figure 1 demonstrates the conclusive observations about this paper which depicts how the proposed algorithm performs in comparison with the standard algorithms. All these percentages are evaluated on a worst case basis, so in actual practice, we should get the given minimum performance boost.

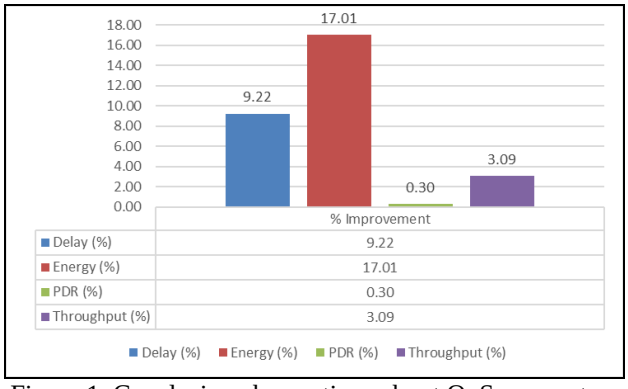

Figure.1. Conclusive observations about QoS parameters

The proposed machine learning based early attack detection algorithm has more than 9% worst case improvement in end to end delay when compared with the best values of the standard algorithms, thus the network will have better communication speed. The proposed network largely improves on the energy consumption of the network, and improves the network lifetime by 17%, which is a big boost for energy constrained networks. The PDR and throughput are improved by 3% and 0.3% respectively. Generally 0.3% improvement in PDR does not look like a large improvement, but in case of high throughput

networks where the number of packets per unit time is more than 1 Million, an improvement of 0.3% accounts to about 3000 packets, which if delivered successfully, would be a big boost for the overall network performance.

5. FUTURE WORK

Due to the emerging nature of blockchain based techniques, researchers can try to integrated blockchain into the proposed machine learning and early attack detection techniques and observe the result improvements in attack detection and removal along with the overall security of the network. This will help the researchers to further study the effects of blockchain in wireless networks and explore more areas in the field of application.

6. REFERENCES

[1] P. H. Yu and U. W. Pooch, "A secure dynamic cryptographic and encryption protocol for wireless networks," IEEE EUROCON 2009, St.-Petersburg, 2009, pp. 1860-1865. doi: 10.1109/EURCON.2009.5167898

[2] S. V. Zareshin, L. I. Shustova and N. Y. Shestakova, "Comprehensive analysis of wireless networks security in moscow central district," 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg, 2017, pp. 240-241. doi: 10.1109/EIConRus.2017.7910537

[3] A. Gupta, O. J. Pandey, M. Shukla, A. Dadhich, S. Mathur and A. Ingle, "Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks," 2013 IEEE International Conference on Computational Intelligence and Computing Research, Enathi, 2013, pp. 1-7.

[4] P. Sankar Chatterjee and M. Roy, "Lightweight cloned-node detection algorithm for efficiently handling SSDF attacks and facilitating secure spectrum allocation in CWSNs," in IET Wireless Sensor Systems, vol. 8, no. 3, pp. 121-128, 6 2018.

[5] P. Casas, A. D'Alconzo, P. Fiadino and C. Callegari, "Detecting and diagnosing anomalies in cellular networks using Random Neural Networks," 2016 International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, 2016, pp. 351-356.

[6] G. Varshney and H. Gupta, "A security framework for IOT devices against wireless threats," 2017 2nd International Conference on Telecommunication and Networks (TEL-NET), Noida, 2017, pp. 1-6.

[7] M. Khalil and M. A. Azer, "Sybil attack prevention through identity symmetric scheme in vehicular ad-hoc networks," 2018 Wireless Days (WD), Dubai, 2018, pp. 184-186.

[8] S. Jha, S. Tripakis, S. A. Seshia and K. Chatterjee, "Game theoretic secure localization in wireless sensor networks," 2014 International Conference on the Internet of Things (IOT), Cambridge, MA, 2014, pp. 85-90.

[9] U. Prathap, P. D. Shenoy and K. R. Venugopal, "PCAD: Power control attack detection in wireless sensor networks," 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Bangalore, 2016, pp. 1-6.

[10] N. Forti, G. Battistelli, L. Chisci and B. Sinopoli, "A Bayesian approach to joint attack detection and resilient state estimation," 2016 IEEE 55th Conference on Decision and Control (CDC), Las Vegas, NV, 2016, pp. 1192-1198.

[11] A. A. Falaye, E. S. Oluyemi, S. Ale, M. B. Abdullahi, U. C. Uchenna and F. Awogbemi, "Quantitative model for dynamic propagation and countermeasure of malicious cyber attack on the mobile wireless network," 2017 Intelligent Systems Conference (IntelliSys), London, 2017, pp. 1095-1102.

[12] V. Nigam, S. Jain and K. Burse, "Profile Based Scheme against DDoS Attack in WSN," 2014 Fourth.