Security Enhancement using Machine Learning Algorithm

Anithaashri TP[1], Baskaran R[2], Ravichandran G[3]

1. Professor, Saveetha School of Engineering, Chennai

2. Professor, Anna University, Chennai

3. Research Scholar, AMET University

Abstract

The security in accessing the data through wireless network is a major task in emerging technology. Since the improvements in the industrial automation are vast, it is in need of reduction in energy consumption, faster accessibility and high security for the transformation of data. To deploy the critical service, in automation process of industrial requirements need the support of highly secured IT management upgrades to handle the application of 5th generation technology with wireless network environment. The novel framework has been designed to provide reigned secured transaction in the wireless network. The implant of centralized control system with machine intelligence maintains secured transactions and operations in the wireless network. In this system the usage of the bio-metric authenticity plays a vital role for unique approach. The novel numerical method is used in machine learning algorithms to solve these problems and provide the security enhancement. The result shows that the novel approach has consistent improvement in enhancing the security in the transactions of data in the next generation technology.

Keywords: bio-metric authenticity, Wireless Network Security, Machine Learning Algorithms

1.0 Introduction

In the wireless network environment, the security in transaction of data through the electronic devices needs to address many challenges in real time situations. The problems of limited resources, less memory, low battery energy, and dynamically changing topology requires the optimal solution for the robustness of data transaction in the wireless network. The model driven engineering in object oriented analysis and design can help in designing the new solutions to the industry related problem. During the transaction of the information, possibility of vulnerabilities such as eavesdropping, denial of service, poor in quality of service, message distortion, nodes roaming in hostile environment, etc. These problems lead to the lavishness in accomplishing the given task in real time situations.

While accessing the information in a wireless mode face the challenges in security. The security issues of wireless network is listed as follows: Firstly, use of wireless link renders network to link attack ranging from passive eavesdropping to active impersonation, message replay, and message distortion. Secondly, poor physical resistance, roaming of nodes in a confrontational environment, have probability of being compromised. Thirdly, due to the frequent presence and absence of the nodes in the network lead to the occurrence of dynamic changes in the transaction of information. Finally, the wireless network may consist of hundreds of nodes, and security mechanisms should be scalable to handle such a large network. Therefore, to provide good successful applications in the wireless network requires high security for authenticated communications.

In wireless network, sending packets from one device to another is done via a series of

intermediate nodes. For a smooth network packet transmission, various kind of routing algorithms are used. The proactive algorithms such as Optimized Link State Routing (OLSR) protocol can be utilised. This algorithm is efficient in bandwidth utilization and in path calculation, it is vulnerable to various attacks like withholding attacks, black-hole attacks, colluding mis-relay attacks, DOS attacks and WoW (Warrior of War) attack, etc. The novel proposal to enhance security in wireless network has been reviewed. The overhead of the additional virtual nodes diminishes as network size increases, which has consistent improvement in enhancing the security in the transactions of data on large networks.

2.0 Related work

In the wireless network environment, accessing the data in a secure [4] manner is a major task. Many protocols have been developed with the limitations in failure detection. The protocols such as gossiping protocol in the multi-level situations, the failure detector was pioneered in [27], and the module is resident at each node in the network. The disadvantage of this protocol is that lack of work while a large percentage of components crash or become partitioned away. In the internet accessibility, the protocol defines a multilevel hierarchy using the design of Internet domains and sub domains as defined by comparing their respective IP addresses. Given two hosts, the longer the common prefix of their IP addresses, the closer they are in the hierarchy. In the failure detection protocol, most gossip messages are sent using the basic protocol[27],[28] within a subnet. Then, fewer gossip messages are sent across different subnets, and even fewer across different domains. The total number of messages can be kept low regardless of the actual network topology [25]. The number of messages at a given domain only depends on the number of subnets in that domain. According to the work in [2], this protocol tolerates lossy communication, although the detection time is affected by the probability of message loss.

In the wireless network, the automation of industrial processes handles the problem of denial of service and the decoupling techniques provides virtual access point abstractions to simplify network management for a wide range of enterprise requirements [3],[4]. In literature [13], the novel structure of neural network has been utilised to detect malicious nodes and limitation with the time consumption. In [14],[15] the concept of game theory has been used such that the zero-sum-game approach helps to the selective node acknowledgements in the forward data path. The robustness of Markov Chain model [19] improves in identifying the cyber attacks in the network, provides the way to detect the problem. In the wireless sensor network, clean slate approach identified to meet the challenges of routing problems during the transmission. The concept of game techniques used to verify availability of the service and addressed the issues denial of service [9], [11] attacks by using the properties of network protocols and thus obtain the solution to control the network. But these solutions are not optimistic for the often usage of protocols in wireless environment. These protocols are very simple but are less efficient in the wireless network, hence made a way to dig the concepts to overcome the limitations and paved the way to use the machine learning techniques for the robustness and in an efficient manner.

3.0 Proposed System

To provide the security to the nodes in the wireless network environment is a difficult

task for multi user accessibility through n-number of electronic devices. There are three level of approaches has been carried out to accomplish the task. Initially, it has been designed for simple node as attacker and defender method. In the later stage, the multi nodes environment handled with the novel numerical approach. Finally, all-in-one model has been developed to address the various kinds of vulnerabilities in multiple situations and optimal solution is obtained.

Monitoring the devices with authenticated accessibility is one of the major task in the recent emerging trends. This paper specifies the significance of monitoring system in distributed environment. By applying mathematical model, the monitoring system works. The systems starts from lower number of devices to high number of devices. The proposed system works according to the user requirements in the distributed environment. In each process will detect the local failure and considered to be a module. Each module will be processed by the monitor system and resolve the problems for good execution. The monitoring system works on the basis of two properties namely precision and prediction. The precision detects the nodes which are in actual vulnerabilities such as sniffing, intrusions, denial of service attack, vampire attack and solves the problem to make the eminent transmission for the proper execution of the device. The prediction specifies the problem that may happen to the device due to the vulnerabilities. Initially the data can be entered using biometric authenticity system. The features are extracted by mapping with the multiple sources using game theory approaches, specifically in terms of strategy analysis method. By using the novel numerical approach with machine learning techniques, the transaction of information will be much authenticated and provides security.

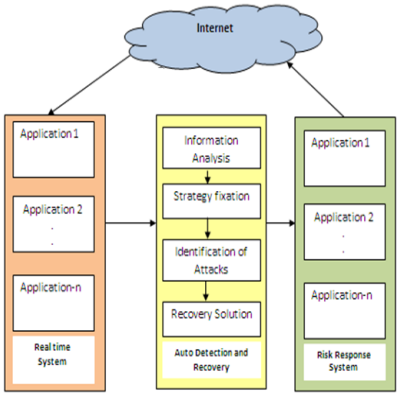

Figure -1 Enhanced Security System

The enhanced security system works on the basis of the machine learning algorithms with numerical approach. The Figure-1 shows the presence and interactions of two nodes over potentially disparate cyber and physical spaces makes the study interesting. Primarily the case of fixed costs and Boolean attack outcomes has been considered, and show that the survival is deterministic even under probabilistic attack and defence strategies. Then, consider more general cases in which the performance is determined by the number of resources deployed by the defender minus that disrupted by the attacker. Hence, an attack may disrupt a subset of the resources, and thus degrade the performance of the system without necessarily bringing it down. For this formulation, the linear, negative exponential and S-shaped benefit functions are deliberated. The conclusions are:

A set of metrics such as reliability, maintainability and availability have been proposed in to quantify the quality of service. Those metrics described the speed ability of the monitor system. The main advantage of this system is the removal of false detection. Due to the analysis of bio-metric authentication in the source node and then mapping takes place.

In some situations the nodes' preferences are most naturally defined not over action

profiles but over their consequences. When building a state of limited competition, for example, consider the set of nodes to be a set of nodes and the set of actions of each user to be the set of transactions.

When each user cares only about the speed of execution of the system for specific transaction, then the model will be formulated as follows :

Function f: A→O (1)

where f is a transition function and O is a set of outcomes and it associates the outcomes with action profiles, and a profile $<P_i^*>$ of preference relations over O.

Then the preference relation P_i of each node i in the strategy of network is defined as follows:

a $<P_i>$ b if and only if f(a) $<P_i^*>$ f(b) (2)

Then the Nash equilibrium of the strategy can be denoted as {N, A_i, (P_i)}, where N is nash equilibrium, A_i is set of actions by the nodes i=1,2,…,n and $<P_i>$ is preference relation.

Suppose the outcome of an action profile is affected by an external variable (v) which is not known to the nodes before it takes the action. To build a model for such a situation novel mathematical strategy can be applied. Let O be the set of outcomes, a probability space SI, and a function (h) is
h:A X SI→ O (3)

with the interpretation that h(a,v) is the consequence when the action profile a € A and the realization of the random variable v € SI.

A set of actions lures a draw on the outcomes O. Then each node i a preference relation $<P_i*>$ must be specified over the set of all such draws. The Node i's preference relation in the strategic analysis is defined as follows:
a $<P_i>$ b (4)

if and only if the draw over the outcomes O lured by h(a,.) is at least as good according to <Pi*> as the draw is induced by h(b,.). The states of the nodes can be handled by two different nets namely Indefinite Key Net and Indefinite Event Net.

Indefinite Key Net is a quadruple (S, T, F, λ) where S is a finite set of states, T is a finite set of moves (S∩T≠Φ), F Contained in or equal to (S x T) U(T X S) is a set of arcs and μ= (μ_1,μ_2,..,μ_n) is a set of triggering states of transitions.

As an extension of Indefinite Key Nets, Indefinite Incentive Net is a powerful graphical and mathematical tool, which not only is able to model concurrent, asynchronous, stochastic and nondeterministic events, but also provide transition enabling function and firing probability that can be used to model various algorithms and strategies.

An Indefinite Event Net is the 9-tuple vector (N,S,T,π, A,I, μ,δ,I_0) where P = 1,2,…,n denotes a finite set of nodes, S is a ¯finite set of states, T = T_1 U T_2 U…U T_n is a finite set of moves, where T_k is the set of transitions with respect to node k, for kϵP, π:T→ [0,1] is a routing policy representing probability of choosing a particular transition, A⊆ J U O is a set of arcs where J **⊆**(P x T) and O ⊆(T x S), such that S ∩ T =Φ and S U T ≠ Φ, I : T→ ($I^{(1)}$;$I^{(2)}$,...,$I^{(n)}$) is a incentive function for the node taking each action, μ = (μ_1, μ_2 ,…,μ_k) is a set of triggering states of transitions in transition set, where k is the number of transitions, δ(s^k_i) is the utility function, when node k in

the condition s_i. Accordingly, the node can choose the best transition, I_0 is the initial marking. The possible strategies existing within the network can be represented in Indefinite Event Net structure.

The algorithm is to find the Nash Equilibrium of an action sequence with π^* for all the nodes. For every leaf node x_i marked by M_i in the reachability tree and a token s such that there is a state p, $T_i(p) = s_i$, $1 \leq i \leq n$ in the reachability tree.

Generally, there are multiple paths from the initial state to a leaf node. Assume x_i is a leaf node, and there are y_i separate paths from the root to xi. Let $t_1^{(i,y)}$,$t_2^{(i,y)}$,…,$t_K^{(i,y)}$, $K=k^{(i,y)}$ be the y^{th} path from root node to leaf node x_i. Define a leaf probability for the leaf node x_i of the y^{th} path as

$$f^{(yt)}(xi) = \pi(t_1^{(i,y)})\ \pi(t_2^{(i,y)}) ,\ldots,\pi(t_K^{(i,y)}) \quad (5)$$

Then the final utility vector for the system is

$$(U1,U2,\ldots,Un) = [\sum_{a=1\ldots yi} f^{(a)}(x_i) * (h^{(a)}(s_i))] \quad (6)$$

where i varies from 1to n and n is the number of leaves in the reachability tree.

Thus, the problem is to find such π that $(U_1,U_2,\ldots,U_n)$ is a Nash equilibrium for each node, which could be given as:

$$\max \prod U = (U_1,U_2,\ldots,U_n) \quad (7)$$

that, the above equation is a multi-objective optimization, which can be solved using the mathematical programming methods.

Results :

The proposed system has been tested with the attack-defend system model which is the most general form among all the network attacks. By testing with the sample network, an attacker will try to intrude a computer system, and the computer takes actions to defend. Assume attacker as Node 1 and the defender as Node 2. By using the above steps, the reachability tree can be drawn and thus the Nash equilibrium can be obtained through the equation (7).

Defender's gain is based on the expected loss by attack and recovery by restore. But attacker's gain is based only on the expected income by attack. On the basis of these ideas, the probability of intrusion will vary from 0 to 1 and it has been tested with various scenarios and tabulated in the following Table-3

Table-1 Analysis on different types of attack

Attack type	Expected loss	Detection rate	Defender's action
http	0.64	0.84	√
ftp	0.27	0.54	T
Web	0.48	0.72	√
WoW	0.55	0.75	T
P2P	0.63	0.73	T

In the above table the tick marks shows clearly that on the basis of the detection rate, the defender's action can be performed successfully, the term T shows that it is in tolerable condition.

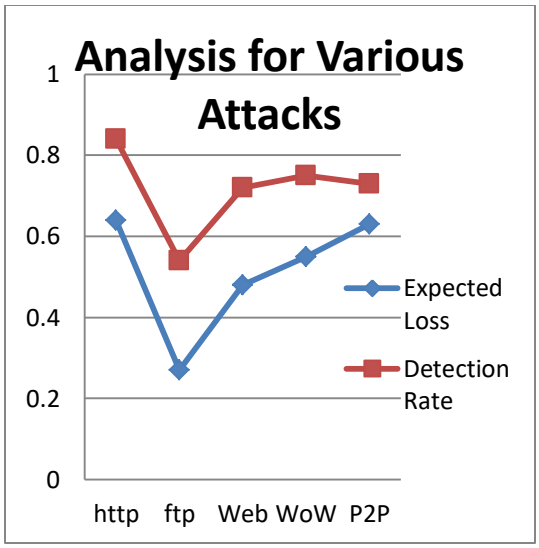

Figure -2 Analysis on different types of Attacks

The Figure-2 shows the improvement in the detection rate, by analyzing on various types of attacks.. Training over imbalanced dataset can lead to skewed models with 10 test beds. To balance the two matrices, by using Equation(6) to calculate the support of each permission in the larger dataset and then proportionally scales down the corresponding support to match that of the smaller dataset. In case that the number of rows of B is bigger than that of M, then the Table-2 specifies utility of the designed system on various sites.

Table-2 Utilisation among various attacks with different sites

Name of the sites	Attack type	RMA	Optimum utilization (Ui)
A	http	1,0,1	0.82
B	ftp	0,0,1	0.64
C	Web	0,1,1	0.72
D	WoW	1,0,0	0.75
E	P2P	1,1,0	0.63

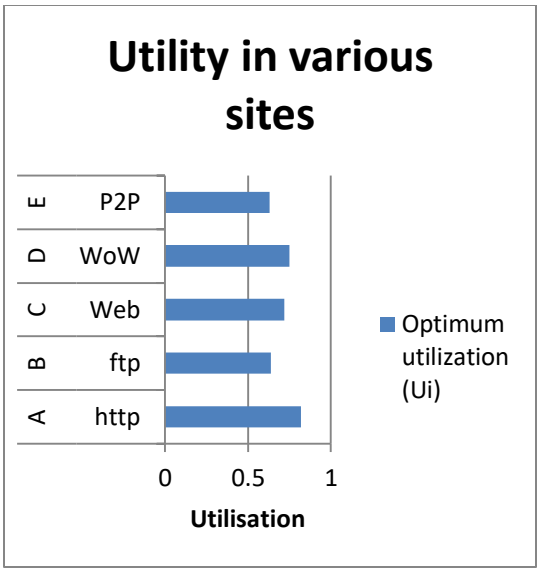

Figure – 3 Utilization on various sites

The Figure-3 shows the utilisation in various cases. In case A, the attack type is of http with optimum utilization. In case B, the ftp attack type is done by the attacker and hence reliability with maintainability exceeds, so that it reduces the utilization of the network. In case C, the attack type is web attack in which all the capability requirements are fulfilled with high utilization. In Case D, the web sniff attack type happens and hence the non-availability and maintainability reflects the dearth in utilization.

It has proved that more detection rate helps in retain ability of the data in the network. and sites since their costs are the same, and the defender defends both, and hence the system survives. In case B, the cyber attack cost is much higher leading a smaller number of server attacks, and consequently, the residual capacity is much higher. In both cases A and B, the proportional defence strategy yields a higher expected capacity. In case C, the cost of site defence is much higher and consequently the defender does not choose to defend the sites.

5 Conclusion

The performance of the novel approach is used to improve the security of wireless network using machine learning technique. The modern numerical approach to find the strategies of nodes, is one of the magnificent methodology to analyse the intrusions in the wireless network. In this paper, the problem of security in the wireless network has been addressed and improvised for the security of the network. It has been started with two player game model, with attacker and defender and extended for multimode environment with 9-tuple indefinite key event. Here, a node (e.g. administrator) can monitor the neighbouring nodes by using novel numerical approach and find the nash equilibrium with mixed strategy. By using this numerical approach the system accepts a simple method with rationality, which helps to analyze the perception of opponent (intruders) with the different factors of indefinite key event vector. The factors are used to observe the strategies of the nodes, calculating their payoffs and the utility function. Thus it gives the high security in the wireless network application and no overhead across the network for the utility of network application. Each new node initially sends its signature, which is later used to validate its information. The countermeasures are imposed to identify and isolate the malevolent nodes and confirm that it does not disturb the regular operations in the network. The framework was tested for various kinds of attacks such as WoW attack, http attack, ftp attack etc. in a multi-user environment, which is a typical repeated network environment with imperfect information strategies in a common defence for the network application. The novel approach has solved the problem of inconsistency such that, each user in the network application requires an individual security strategy to satisfy its own target, and these strategies need to be optimized to get the perfect solution for the transaction of information through wireless network. Thus, by applying novel numerical approach with the machine learning technique to determine the classification and decision making which enable to find the optimal solution to give the high end security to the network accessibility.

6 References :

[1] Ming Wan, Jiangyuan Yao, Yuan Jing and Xi Jin,(2018) Event based anamoly detection for Non-Public Industrial Communication Protocols in SDN based control systems. *CMC, vol.55, no.3, pp.447-463, 2018*

[2] Alexey G.FinogeevAnton A.Finogeev, (2017) "Information attacks and security in wireless networks of industrial SCADA systems", Journal of Industrial Information Integration, Volume 5, March 2017, pp. 6-16 //doi.org/10.1016/j.jii.2017.02.002

[3] Anithaashri TP and Baskaran R, (2016) "Enhancing multi-user network security using sagacity and dismissal of conquered movements" in the International journal on Computational and Theoretical Nanoscience, Vol-13, No.1, ISSN :1546-1955 Jan, 2016 pp : 69-78

[4] Parli B. Hari ; Shailendra Narayan Singh, (2016)"Security issues in Wireless Networks: Current research and challenges **"** International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring), 8-9 April 2016, DOI**:** 10.1109/ICACCA.2016.75788764

[5] Zhou, C.; Huang, S.; Xiong, N.; Yang, S.; Li, H. et al. (2015): Design and analysis of multimodel-based anomaly intrusion detection systems in industrial process automation. *IEEE Transactions on Systems Man & Cybernetics Systems*, vol. 45, no. 10, pp. 1345-1360.

[6] Goldenberg, N.; Wool, A. (2013): Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. *International Journal of Critical Infrastructure Protection*, vol. 6, no.2, pp. 63-75.

[7] E. Haleplidis, S. Denazis, K. Pentikousis, J. H. Salim, O. Koufopavlou, Sdn layers and architecture terminology, Tech. Rep. 01 (2013).

[8] TP Anithaashri and R Baskaran, (2012) "Enhancing the Network Security using Amalgamation" in International journal on Cryptography and Information security, Vol-2, No.1, Mar, 2012 pp: 226-234

[9] H. Beitollahi, G. Deconinck,(2012) "Analyzing Well-Known Countermeasures against Distributed Denial of Service Attacks", Journal of Computer Communication, 35(7) 759-771.

[10] Anithaashri T.P., Baskaran R. (2012) Enhancing the Network Security Using Lexicographic Game. In: Meghanathan N., Chaki N., Nagamalai D. (eds) Advances in Computer Science and Information Technology. Computer Science and Information Technology. CCSIT 2012. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 86. Springer, Berlin, Heidelberg

[11] H. Beitollahi, G. Deconinck, (2011) "A Cooperative Mechanism to Defense against Distributed Denial of Service Attacks", Proceeding Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-11) Vol. 1,pp: 11-20.

[12] Zhen Yu, Young Guan,(2010), "A dynamic en-route filtering scheme for data reporting in wireless networks" in IEEE/ACM transactions on networking Vol.18, No.1, February 2010.

[13] Linda O, Vollmer T, Manic M. (2009): "Neural network based intrusion detection system for critical infrastructures". *International Joint Conference on Neural Networks*, pp. 1827-1834.

[14] T.P.Anithaashri, G.Ravichandran, R. Baskaran,"Security Enhancement for wireless network communication", IEEExplore Digital Library, ICOEI, 11-12, May,2018 **DOI:** 10.1109/ICOEI.2018.8553735