International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 08, 2020
ISSN: 1475-7192

Security Enhancement in Wireless Sensor Network using Sagacity Dismissal of Conquered Movements

[1]T.P.Anithaashri, [2]P.Selvi Rajendran, [3]G.Ravichandran

ABSTRACT--*Wireless Sensor Network (WSN) is a new approach for network programmability, which refers to the ability to control, change, and manage network behavior dynamically through sensor via open interfaces in contrast to relying on closed boxes and proprietary defined interfaces. It envision the plan, deploy the critical service, performance and industrial management upgrades for the utilization of 5th generation technology. The WSN framework enables centralized control of data path elements independently of the network technology used to connect these devices that can originate from different vendors. The centralized control embeds all the intelligence and maintains a network wide view of the data path elements and links that connect them. This sensor based network makes the controller suitable to perform network management functions while allowing easy modifications to the networking functions through the centralized control plane. To meet the vast requirements it is mandatory to enhance the technology in the network application, for which the software defined network can be very essential to meet the challenges in the technical advancement for rendering and utilizing the services. 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.*

Keywords--*Security Enhancement in Wireless Sensor Network using Sagacity Dismissal of Conquered Movements*

I. INTRODUCTION

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.

[1] *Associate Professor, Department of Innovative Informatics, Institute of Computer Science Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, shri3krra@gmail.com, anithaashritp.sse@saveetha.com*

[2] *Professor, Department of Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai, selvir@hindustanuniv.ac.in*

[3] *Research Scholar, AMET,Chennai, vpigcet@gmail.com*

Received: 21 Dec 2019 | Revised: 18 Jan 2020 | Accepted: 05 Feb 2020

II. EXISTING SYSTEM

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 [3] 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 [10] 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. 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.

Recent developments in the field of materials science and solid-state physics are also important in that respect. They could give information appliances and computers of the future a completely

different shape, or even mean that computers will no longer be recognizable as such because they

will completely blend into their surroundings. The displays of micro-electronic devices could be configured to present information in bad weather, traffic or sports results extracted from the Internet. Once configured, users could place these displays wherever they felt it was convenient. As humans, it need to be accustomed for looking in pieces of information [13]. This way, dynamic information would become much easier to find and assimilate.

III. PROPOSED SYSTEM

Given the continuing technical progress in computing and communication, it encompasses the use of networks and computing power. The computer as a dedicated device should be invisible, while at the same time making its data processing capabilities available throughout environment. Intrusive technology should make way for “silent technology”:

The effects of rapid progress in microelectronics and the convergence of communications and

information technology can be demonstrated using the5th generation technology. A few years ago, mobile phones were still so big, expensive, and limited in their functionality that they didn't sell very well and were often used more as a status symbol than a practical tool. This has changed very rapidly. Many users have grown so accustomed to mobile phones and adapted their professional or even private lives to them that they can't imagine life without this technology. Parallel to this development, within a short period of time the mobile phone has become a device that offers more than just the pure functionality of voice transmission. The SMS short messaging system has become a completely unexpected success. Cameras and colored displays, which permit the viewing of forwarded photos and video clips, are now being integrated into most mobile phones. The same applies to functionality that offers high-quality music reproduction, bulk data transmission, etc. The prices for microelectronic functionality with the same amount of computing power are falling radically over time. Technology experts expect this way to continue for more years to come, meaning that computer processors and storage components will be more powerful, smaller, and cheaper than any other technology. The Wireless Sensor

Network plays a vital role in improvising the security in the data transmission and other applications. The overview of the security in WSN has been deployed in figure-1.

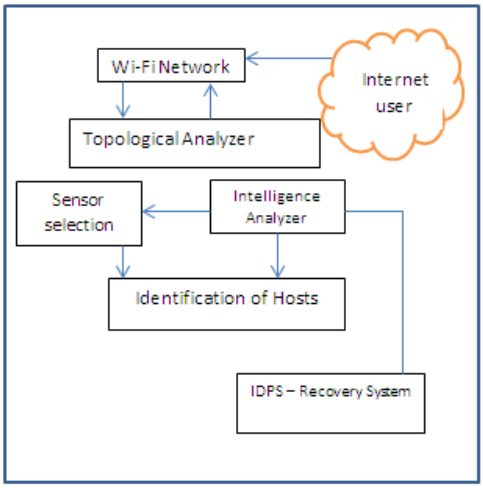

Figure – 1 Security in WSN

Even if a detailed assessment cannot yet be made of these, it is clear that completely new applications will come into existence based on this multimode operations. It seems to be the ubiquitous computing in general will, run in a better way to have dramatic economic effects: In many new services it is possible that transformation of the huge amount of information gathered by the smart devices brought out for the human user. The maintenance and ongoing development of the global infrastructure necessary for cooperating and communicating smart 5^{th} generation technical objects – including the measures required to meet requirements for high security and privacy in such an environment which might eventually occupy a whole industry, similar to today's energy and telecommunications enterprises. The sagacity dismissal of conquered movements of numerical logic works to identify the intruder and dominates the defend action [3].

An Indefinite Event Net is the 9-tuple vector $(N,S,T,\pi, A,I, \mu,\delta,I_0)$ where $P = 1,2,\ldots,n$ denotes a finite set of nodes, S is a ¯finite set of states, $T = T_1 \cup T_2 \cup \ldots \cup T_n$ is a finite set of moves, where T_k is the set of transitions with respect to node k, for $k \epsilon P$, $\pi: T \rightarrow [0,1]$ is a routing policy representing probability of choosing a particular transition, $A \subseteq J \cup O$ is a set of arcs where $J \subseteq (P \times T)$ and $O \subseteq (T \times S)$, such that $S \cap T = \Phi$ and $S \cup T \neq \Phi$, $I : T \rightarrow (I^{(1)};I^{(2)},\ldots,I^{(n)})$ is a incentive function for the node taking each action, $\mu = (\mu_1, \mu_2 ,\ldots,\mu_k)$ is a set of triggering states of transitions in transition set, where k is the number of transitions, $\delta(s^k_i)$ 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.

Received: 21 Dec 2019 | Revised: 18 Jan 2020 | Accepted: 05 Feb 2020

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 $t_1^{(i,y)}, t_2^{(i,y)}, \ldots, t_K^{(i,y)}$, $K=k^{(i,y)}$ 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

$$f^{(yt)}(xi) = \pi(t_1^{(i,y)})\ \pi(t_2^{(i,y)}) ,\ldots,\pi(t_K^{(i,y)}) \quad \text{---- (1)}$$

Then the final utility vector for the system is

$$(U1,U2,\ldots,Un) = [\sum_{a=1\ldots yi} f^{(a)}(x_i) * (h^{(a)}(s_i))] \text{ --- (2)}$$

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:

$$\max \prod U = (U_1,U_2,\ldots,U_n) \quad \text{----(3)}$$

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

IV. RESULTS

The proposed system has been tested with the attack-defend system model which is the most general form among all the network attacks. In a basic attack-defense cast, there are two nodes, the defender and the attacker. For easy to illustrate, choose a simple attack case in this subsection. Here an attacker will try to intrude through a host, and the system takes actions to defend. 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. By using this numerical approach with the nash equilibrium 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.

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 : 69-7

Received: 21 Dec 2019 | Revised: 18 Jan 2020 | Accepted: 05 Feb 2020

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. T.P.Anithaashri, G. Ravichandran, R.Baskaran, Software Defined Network Security enhancement using Game Theory, Elsivere COMNET, vol157, pp:112-121, 2019
6. P.Selvi Rajendran,"Virtual Information Kiosk Using Augmented Reality for Easy Shopping",International Journal of Pure and Applied Mathematics (IJPAM). special issue.Volume 118 No. 20 2018, 985-994,Scopus
7. T.P.Anithaashri, G. Ravichandran , et.al. Secure Data Access Through Electronic Devices Using Artificial Intelligence, ICCES, 2018
8. T.P.Anithaashri, R. Baskaran, Enhancing Multi-user Network using sagacity dismissal of conquered movements, International Journal of American Scientific Publishers pp:69-78, 2016
9. TPAnithaashri and R Baskaran, Reign Monitor service for web enabled distributed system in the International journal on Computation of Power, Energy, Information and Communication,Vol-12 April 2013
10. TPAnithaashri 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
11. 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
12. Zhen Yu, Young Guan,(2010), "A dynamic en-route filtering scheme for data reporting in wireless ntworks" 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. Yenumula B Reddy, S Srivathsan,(2009) "Game Theory Method for selective forward attacks in wireless networks" in 17th Mediterranean Conference on Control and automation Makedonia Palace, Thessaloniki, Greece. June 24-26,2009.
15. Wei He Chunhe Xia cheng Zhang Yi JiXinyi Ma (2008) – A Network Security Risk Assessment framework based on Game Theory. School of Computer Science and Engg. Beihang University. IEEE DOI 10.11.09/FGCN– `IEEE & CSI Jnl.
16. Min-kyu-Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim (2008), "Wireless Network Security: Vulnerabilities, Threats and Counter measures". International journal of Multimedia and Ubiquitous Engineering Vol.3, No. 3, July 2008
17. B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure Sensor Network Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf., 2006.
18. A Mahimkar and V. Shmatikov,"On the advantage of network coding for improving network throughput" In Proceedings of 18th IEEE computer Society Foundations Workshop, 2005.

19. Nong Ye Sr.MemberIEEE,Yebin Zhan, Connie M Borror "Robustness of the Markov-Chain Method for Cyber-Attack Detection", IEEE transactions on reliability, Vo l53, No.1 March, 2004
20. B. Parno, M. Luk, E. Gaustad, and A. Perrig, (2006)"Secure Sensor Network Routing: A Clean-Slate Approach," CoNEXT: Proc. ACM CoNEXT Conf.
21. A.Mahimkar, V.Shmatikov(2005), "On the advantage of network coding for improving network throughput" in Proceedings of 18th IEEE computer Society Foundations Workshop