ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 3, March 2020

Securing Industrial IoT Networks by Energy Efficient and Reliable Routing Protocol

Latha Murugan[1], Manikandan Chinnaswamy[2]

Department of Applied Electronics, Arunai Engineering College, Thiruvannamalai, Tamil Nadu, India [1]

Assistant Professor, Department of ECE, Arunai Engineering College, Thiruvannamalai, Tamil Nadu, India [2]

ABSTRACT: Industrial IoT (IIoT) refers to the application of IoT which can be characterized as a vast number of connected industrial systems that are communicating and coordinating their data analytics and actions to improve industrial performance. As the number of connected devices and system increases, attack surfaces for data breaches or ransomware becomes greater than ever before. They should ensure an integrated network will not be compromised with consistent data breaches. This paper proposes an Energy Efficient Routing Protocol(E2R2) for transmitting periodic packets on industrial wireless sensor networks. In case of attacks encountered, the protocol paves way to choose alternate path between source and destination nodes. The simulation results show better performance in terms of reliability, throughput and energy consumption.

KEYWORDS: Energy Efficient Reliable Routing, Industrial IoT, Reliable Data Transmission, less Energy consumption.

I. INTRODUCTION

Industrial IoT is a revolutionary attempt to build smart manfacturing eco-system by applying the benefits of IoT to industrial process management. The smart connected devices such as sensors, actuators, and controllers together make up a smart manufacturing enterprise to improve efficiency and profitability.

IIoT is a rapidly evolving and serves several industries and services[1]. Health care systems are equipped with IoT devices which enables sensing, tracking and monitoring of patients, machines and drugs [2]. In agriculture industry, IoT devices are used for effective watering of plants, surveillance of farming lands and storage management of products [3]. Transportation and logistics play a significant role in the supply chain industries. Iot devices are used to find the location of vehicles, to track their movements, and to predict the time of supply [4]. IP-connected cameras, sound sensors are widely used in security and surveillance [5]. IIoT in energy sector manages the supply to and from the grid, leakage monitoring and billing [6]. IoT devices play an important role in the mining industry for sensing disaster signals, managing warning systems, tracking movement of underground miners, and monitoring shipments [7].

The vital part of an automated industry is the Industrial Control System(ICS) which may include Supervisory Control and Data Acquisition(SCADA) networks and Programmable Logic Controllers(PLC). The replacement of conventional electromechanical control systems by embedded devices has given attractive entry points for cyber fraudsters. Cyberattacks such as the stuxnet attack against the nuclear systems of Iran [8], German steel mill blast furnace attack [9], Saudi Aramco oil company attack [10], and Mirai [11]are typical examples of the attacks related to the industrial automated systems. The inclusion of IP connected devices provides good opportunities to attackers in industrial automated systems.

Sensor nodes in an IIoT network produces data at high speed. They communicate this data to base station for processing. They also communicate with other sensor nodes for transmitting synchronized data to base station. The energy is spent in

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 3, March 2020

both transmission and reception of messages amongst the nodes should be minimized. Sensor nodes should be clustered together in an effective manner so that their messages are transmitted jointly and the network lifetime is increased [12].

LEACH is a hierarchical routing protocol which involves clustering of devices for transmitting data to the base station. Cluster heads are responsible for data aggregation, data processing and data communication. The protocol involves randomized cluster head rotation for distribution of routing load among multiple users. LEACH is one of the most widely adopted energy efficient routing algorithms and we treat it as baseline of our approach [12].

Location based routing protocols address sensor nodes by their locations. This is made possible through various techniques including relative distance estimation using signal strengths or information exchange and GPS based location tracking. Flat routing protocols are data centric, which implies that there are no stringent constraints on the original data. Sensor nodes in such protocols co-ordinate to perform data sensing and data is queried by the base station by different geographical areas. High energy nodes are assigned with the task of data processing and transfer of data, where low energy nodes are assigned with sensing [12].

The simulation shows the generation of cluster nodes at first and packet is transferred from source to destination node. Whenever the packet lost due to sinkhole attack, the information is passed to the trust node. Trust node assigns fake designation node and alternates the path between source and destination. Finally, all the packets are successfully transmitted to the base station with reliable data and increased network lifetime.

II. RELATED WORKS

In this section, we present a brief description of the important security frameworks for industrial automation systems and IoT network by describing vulnerabilities and securing from such attacks. C.Nagarajan *et al.*[4] [11] [16] proposed security in power system control networks. They propose an analytical method for measuring the severity of vulnerabilities. Different possibilities of security breaches are mapped into a tree structure and upper bound of threat value is imposed to find pivotal leaves which requires counter measures. Patel et al. [14] developed a vulnerability tree of an industrial control system based on the past history of attacks. For each system in the network, they used two indices, referred as threat impact index and cyber vulnerabilities, both ranging from 0 to 100 and denoting the financial impact and vulnerability impact, respectively. However, these values were assigned using the questionnaire methods. C.Nagarajan *et al.*[11] proposed IoT search engine used for scanning of the vulnerabilities in the IoT devices. The work also analyzes the scan results and discusses the ease of hacking of the IoT devices. However, it does not discuss any method to improve the security of the system. The IoT devices are designed with a capability of communication among them. These cross-dependencies among the IoT devices can be used by an attacker to advance through the network by exploiting the vulnerabilities residing in them.

R.M. Jose et al. [16] proposed a security evaluator referred as C-SEC. Even though the tool is proposed for IIoT networks, their work is focused only on ICSs, and the contribution to the IIoT network is limited. Furthermore, their work is theoretically formulated and no experimental evaluation is conducted. Wang et al. [17] proposed a graphical methodology to find the optimal attack path based on the maximum flow network. They calculated the cost of the attacks through their own methodology. However, they do not evaluate their methodology for a proper IIoT scenario even though their proposal is for IIoT network. Moreover, they do not propose any techniques to mitigate the risk. Vidushi et al. [18] proposed a model which improves the energy constraint problem of devices used in IoT applications. This involves clustering process, cluster head selection and choosing least energy consuming path between transmitter and receiver. They also used sleep scheduling process for enhancing network efficiency. sleep scheduling combines the advantage of particle swam optimization and genetic algorithm. They also compared their performance with LEACH and FCM. Rafe et al. [19] proposed Location based Energy-Aware Reliable routing (LEAR) protocol for wireless sensor networks based on sensor position and clustering. Geographical routing protocols are well known for optimum energy consumption and bandwidth utilization. They also proposed enhanced greedy forwarding for improving lifetime of network. They have demonstrated the simulation results showing extended lifetime for wireless sensor networks.

III. PROPOSED FRAMEWORK

The proposed protocol E2R2(Energy Efficient Reliable Routing protocol) begins with first proces, self organisation phase. In this, after the random distribution of sensor nodes in the network, self-organization phase begins. During the phase clusters are formed using LEACH protocol. The CH set, the current CH, and the two DCH nodes are selected by the Base Station(BS). Each node broadcasts its three attributes namely, geographical location information, residual energy level and velocity or mobility of nodes. This broadcast is related to BS for the selection of CH and CH panel [20].

The location information of nodes are gathered by using GPS. By having the location inforamtion we can perform data dissemination using LBDD(Line-Based Data Dissemination)protocol. This protocol contains two main steps: (i)Dissemination:when the sensor node generates new data, it forwards the data to nearest inline node. (ii)collection: in order to receive any specific information data, sink sends query to the line in a perpendicular fashion [21].

The set of kNNs and their locations may change over time as the node moves. The basic idea of kNN query processing is to collect relevant from the sensor nodes near the query point. As our approach is mainly concerntrated on reduced energy consumption, kNN query processing is a suitable one [22].

Sinkhole attack is an attack were an attacker make vulnerable node to attract all the traffic from the neighbour nodes based on routing metrics used by routing protocol.since communication in WSN are many to one, each node broadcasts it to BS. Thus it launches sinkhole attack. If a sinkhole attacker node is deployed successfully, there will be three possibilities: messages may be lost(dropped by the attacker node), messages may be delayed or messages may be modified.on the basis of three observations, three types of sinkhole attack are possible:

- Sinkhole message modification nodes (SMD): sinkhole attacker nodes modify the messages before forwarding them to the next node.
- Sinkhole message dropping nodes (SDP): sinkhole attacker nodes drop the messages, even sometimes selectively.
- Sinkhole message delay nodes (SDL): sinkhole attacker nodes cause delay in forwarding the messages.

when the node detects the sinkhole attack near its neighbour, it forward to trust node and the trust node provides secure alternative path to the sink [23]. In the detection of sinkhole attack process, any deviation on network behaviour is collected like node id , time of attack etc., by watchdog route monitoring scheme. The preventer node continously watch all the neighbour nodes and real time activity. If it detects any misbehaviour like data forwarding error and continous packet drop, it blocks the attacker and forward the attacker information to all the nodes [24].

IV. SIMULATION RESULTS

The simulation of our proposed work initially shows the formation of cluster nodes in the sensor field. Then packets are routed from the corresponding source to the destination nodes. In between the transmission, the intermediate nodes present among the source and destination nodes analyzes for the secure path whichis nothing but free from sinkhole attacks. The sensor nodes provide fake designation when it exposes to sinkhole attack and alternate route for designation is chosen.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 3, March 2020

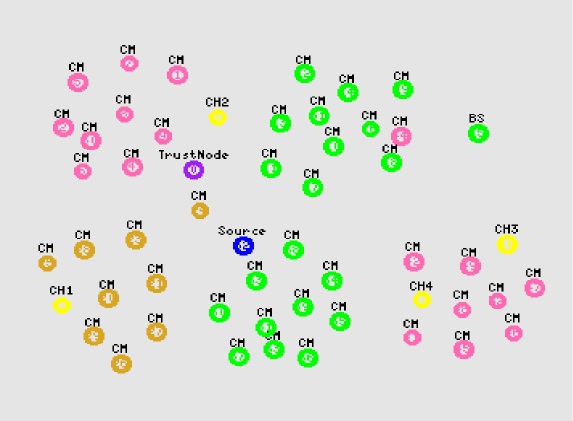

Figure 3: cluster formation

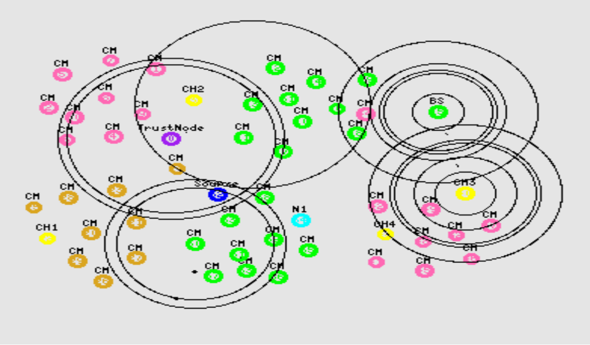

Figure 4: packet transmission between the nodes

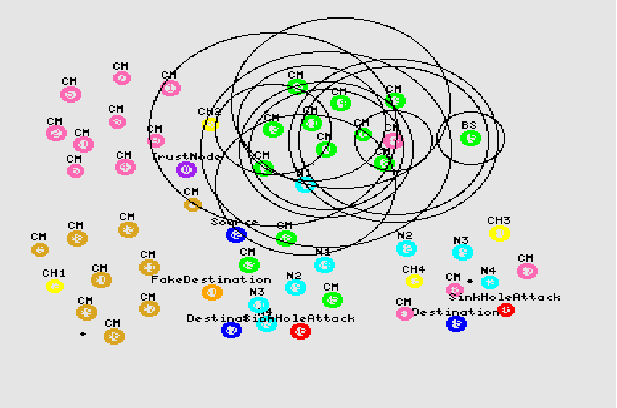

Figure 5: Analysis of sinkhole attack in cluster 2

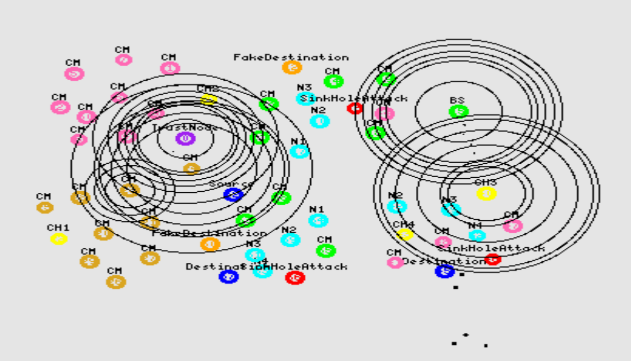

Figure 6: Analysis of sinkhole attack in cluster 3

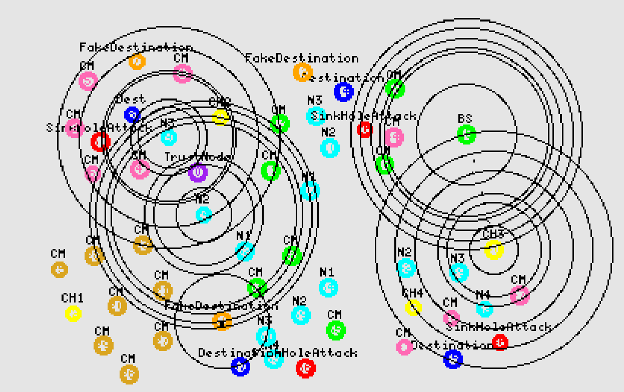

Figure 7: Analysis of sinkhole attack in cluster 4

V. CONCLUSION

In this paper, security data breaches like sinkhole attacks in the industrial IoT networks are identified and solutions to such attacks are provided. The kNN query processing enables gathering of neighbor node location information. If the network analyzes the sinkhole attack, it passes this information to trust node. Trust node assigns fake designation and provides alternate secure route. We have used Energy-Efficient Reliable Routing protocol by using this, packets are transferred with minimum energy consumption and network lifetime is increased. The proposed framework provides better performance in terms of throughput, packet drop rate, delay and residual energy.

REFERENCES

[1] L. Da Xu, W. He, and S. Li, “Internet of things in Industries: A survey”, IEEE Transcations on industrial informatics, vol. 10, no.4, pp.2233-2243, 2014.

[2] Z. Pang, Q. Chen, J. Tian, L. Zheng and E. Durova, “Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet of things”, in Advanced Communication Technology (ICACT),2013 15th International conference on, IEEE, 2013, pp.529-534

[3] Z. Pang, Q. Chen, W. Han, and L. Zheng, "Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion", Information Systems Frontiers,vol.17, no;2, pp.289-319,2015.

[4] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- *Electric Power Components and Systems*, Vol.39 (8), pp.780-793, May 2011

[5] C. Long, Y. Cao, T. Jiang and Q. Zhang, "Edge computing Framework for cooperative video processing in multimedia IoT systems", IEEE Transcations on Multimedia, 2017.

[6] Y. Saleem, N. Crespi, M.H. Rehmani, and R.Copeland, "Internet of things-aided smart grid: technologies, architectures, applications, prototypes and future research directions", arXiv preprint arXiv:1704.08977, 2017.

[7] W. Qiuping, Z. Shunbing, and D. Chunquan, "Study on key technologies of internet of things perceiving mine", Procedia Engineering, vol.26, pp.2326-2333,2011.

[8] J.Y. Keller and D.Sauter, "Monitoring of stealthy attack in networked control systems", in control and Fault-Tolerant systems (SysTol), 2013 Conference on. IEEE, 2013, pp.462-467.

[9] Lee, Robert M and Assante, Michael J and Conway, Tim, "German Steel mill cyberattack", Industrial control systems, vol.30, 2014.

[10] J. Leyden, "Hack on Saudi aramco hit 30,000 workstations, oil firm admits," The register, vol.29, 2012.

[11] E Geetha, C Nagarajan, "Induction Motor Fault Detection and Classification Using Current Signature Analysis Technique", 2018 Conference on Emerging Devices and Smart Systems (ICEDSS), 2nd and 3rd March 2018, organized by mahendra Engineering College, Mallasamudram, PP. 48-52,2018

[12] Myung Kyun Kim and H.P. Ngo, "A Reliable and energy efficient routing protocol in industrial wireless sensor networks", The 2011 International conference on Advanced Technologies for Communications (ATC 2011), Da Nang, 2011, pp.32-35.

[13] C.W. Ten, C.C. Liu and M. Govindarasu, "Vulnerability assessment of cybersecurity for SCADA systems using attack trees", in Power Engineering Society General Meeting, 2007, IEEE, 2007, pp.1-8.

[14] S. Patel and J. Zaveri, "A risk assessment model for cyber attacks on information systems", Journal of Computer, vol.5, no.3, pp.352-359,2010.

[15] J. RomeroMariona, R. Hallman, M. Kline, J. San Miguel, M. Major and L.Kerr, "Security in the internet of things-the C-sec approach", in the proceedings of the International Conference on the Internet of things and Big data, vol.1, 2016, pp.421-428.

[16] C. Nagarajan, M.Madheswaran and D.Ramasubramanian- 'Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model'- *Acta Electrotechnica et Informatica Journal* , Vol.13 (2), pp.18-31,April-June.2013