International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 5 May 2022, pp: 284-288 www.ijaem.net ISSN: 2395-5252

A crossbreed protectedrouting and monitoring structure in IoT-based wireless sensor networks

Mrs. C. NithyaPraba, Dr.D.Kalaivani

Research Scholar (FT) Department of Computer Science Dr.SNSRajalakshmi College of Arts and Science, Coimbatore-49.

Associate Professor & Head Department of Computer Technology Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore - 49.

Submitted: 01-05-2022 Revised: 04-05-2022 Accepted: 08-05-2022

ABSTRACT:
Internet of Things (IoT) has advanced its ubiquity across the world for the expansion of smart networks. It is aimed to dispose network bound that permit smart services and computing for the IoT devices. In addition, this distribution would not only improve the user knowledge but also provide service flexibility in case of any adversity. In IoT applications, the margin computing deed assigned architecture and closeness of end-users to provide faster response and better quality of service. However, the security regard is mainly transmit to resist the vulnerability of attacks (VoA). Existing methodologies deal only with static wireless sensor web to deduce the intrusions in which the sensor nodes are deployed in a uniform manner to retain the constancy. Since the sensor nodes are constantly being in question through different transmission regions with several levels of velocities, selection of sensor monitoring nodes or guard nodes has become a challenging job in recent research. In addition, the adversaries are also moving from one location to another to explore its specific chores around the network. Thus, to provide flexible security, we propose a secure routing and monitoring protocol with multi-variant tuples using Two-Fish (TF) symmetric key approach to discover and prevent the adversaries in the global sensor network. The proposed approach is designed on the basis of the Authentication and Encryption Model (ATE). Using Eligibility Weight Function (EWF), the sensor guard nodes are selected and it is hidden with the help of complex symmetric key approach. A secure hybrid routing protocol is chosen to be built by inheriting the properties of both Multipath Optimized Link State Routing (OLSR) and Ad hoc On-Demand Multipath Distance Vector (AOMDV) protocols. The result of the proposed approach is shown that it has a high percentage of monitoringnodes in comparison with the existing routing schemes. Moreover, the proposed routing mechanism is resilient to multiple mobile adversaries; and hence it ensures multipath delivery.

Keywords:vector,protocols,cyber-attacks,routing.

I. INTRODUCTION:

IoT is widely accepted as a 3rd industrial revolution that embeds the computing object to send and receive the physical data over the Internet [1], [2]. It is uprising at breathtaking-pace, initiated with 2 billion physical objects in 2006 into 200 billion by 2020 [3] i.e. growth of 200%. IoT devices / sensors generally collect and observe the temporal/spatial information to manage the real-time events addressing various challenges [4], [5]. IoT applications are becoming smarter for various applications namely education, finance, energy, healthcare, transportation and smart cities [6]. Subsequently, academia, industry and individuals are enduring to provide security and safety i.e. for IoT devices and networks. These factors should chiefly be concerned to avoid data catastrophe to the IoT users. For example, a smart home system can be monitored remotely by the cyber-attackers, and smart vehicle communication can be seized to create a source of danger among the citizens. This catastrophe condition is highly exposed to Internet-connective objects to affect the IoT security systems and ecosystems of complex communication networks such as social networks, application, websites and Robo networks i.e. botnet.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 5 May 2022, pp: 284-288 www.ijaem.net ISSN: 2395-5252

In contrast, cooperating a single communication channel or component can make the IoT-based system powerless as a part or complete network access. Dyncyberattack gathered the connective device to install within smart cities and gathered them as botnets i.e. Zombie Army through middleware known as Mirai in 2016. In addition to the vulnerabilities, the IoT system is now evolving of attack vectors in terms of diversity and complexity. Therefore, Wireless Sensor Networks (WSN) is considered as a set of resources that impels sensor nodes to gather data from the environment; compute the collected outputs into a formatted data, and transmit it to the destination terminal through the wireless medium. The source of input will be the sensed information gathered from different types of sensors such as temperature, pressure, magnitude, level and flow sensors and so on. The open nature of the wireless medium makes the network weak and defenseless to protect its data from adversaries when compared to the strongly built infrastructure wired networks.

WSN [7] provides valuable communication in the battle fields or defense-oriented applications to recover out the lights, electromagnetic signals, chemical or biological vapors, and the enemy presence or border violations. Providing security with optimized energy in WSNs is a hard job when nodes are in motion. Because managing the localization of sensor nodes and moving adversaries are the decisive one in terms of protective factors. There are dissimilar cases of attacks created by the adversaries depends on their objectives or without any motives [8]. Any wireless sensor node equipped with sufficient hardware and software can act as an adversary to sense the wireless channel to grab the transmitting data in an unauthorized way. In addition, the adversaries may try to change the natural behavior of the normal sensor nodes and compromise it to violate the activities of the wireless sensor network and this will make the sensor nodes to downhill on their performance, throughput, and service [9].

To infer these vulnerable activities or attacks, Intrusion Detection System (IDS) is used in practice. The IDS [10], [11], [12] is mainly used in wired networks with the deployment of hardware systems between servers or nodes to monitor the network activities. In literature, IDS based learning mechanisms have been considered for the evaluation of traditional network systems i.e. not specifically for IoT systems [13], [14], [15], [16], [17], [18]. Agarwal et al. [13] reviewed various data mining techniques for network anomaly detection. Buczak et al. [14] explained the data mining and machine learning methods to show the significance of cyber analytics in the endurance of intrusion detection and prevention. These survey papers provided substantial references to summarise the challenges of cyber securities.

Even though, Fadlullah et al. [17] focused on deep learning mechanism to study the traffic-control systems. Hodo et al. [18] presented taxonomy of deep and swallow networks to survey on intrusion detection and prevention systems. In addition, Wang and Jones [15] reviewed data mining, machine learning, deep learning, and bid-data to evaluate the criteria such as data streaming, processing, reduction and feature characteristics. Mishra et al. [16] compared and examined the limitation and constraints of machine learning techniques to analyze intrusion detection. Table 1 shows the important notation used in this paper.

The existing survey targets IDS and IoT to identity two basic state-of-the-arts such as an overview of IoT, IDS, and classification of taxonomy [19], [20]. In addition, they proposed a detailed survey to compare the different detection and prevention system i.e. for IoT to analyze the parameters such as detection approaches, validation strategies, and placement schemes. Though, BenKhelifa et al. et al. [19] focused on the advancements of detection and prevention practices in IoT. They surveyed the recent state-of-the-art approaches with a special reference on IoT architecture. In random Ad hoc sensor networks, the sensor nodes are presented in a distributed manner without any centralized equipment and it is widely known to be a Distributed Intrusion Detection System (DIDS) [21]. Since then, several DIDS schemes [22], [23], [24] have been presented to discover and forestall the attacks in random sensor networks. The purpose of the schemes was to select watchdogs or monitor nodes to protect the wireless sensor network. Hither, to detect the attacks, the safeguard nodes are selected from neighbor nodes.

For data transmission and monitoring purpose, the sensor node has two selective approaches, namely Hierarchical or Clustered and Flat or Random. In the cluster approach [25], [26], the sensor nodes are used to form as clusters; and thus it will elect its cluster head for each cluster using any leader election algorithm. By then, the cluster head will act as a monitor node to the local cluster and it will help to detect the availability of the unauthorized traffics or intruder nodes in the cluster. Eventually, it will share the detection reports between the monitor nodes or other cluster heads to deliver to a base station (BS). Then, it will start the fault recovery process at the necessary

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 5 May 2022, pp: 284-288 www.ijaem.net ISSN: 2395-5252

links or nodes through the BS. In each round time execution, the cluster head will be selected by the election scheme which will later create a computation overhead to the sensor networks. Moreover, each cluster will be monitored by a single cluster head that may cause a single point failure. In the random approach [27], few wireless sensor nodes are randomly selected based on neighbor locations or hops.

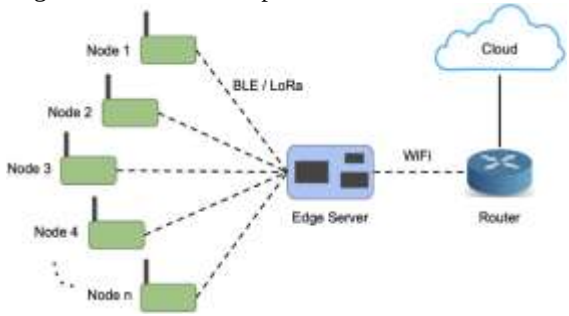


Fig:IoT monitoring in routing.

The selected nodes are eligible to monitor the nearest sensor nodes within the accessible transmission range. This random approach is suitable to elect the nodes in Ad hoc sensor networks. In both of the approach, the selection of safeguarding nodes is open in the wireless medium; and thus the security scheme is being challenged to ensure the channel privacy. The recent approaches use the key management technique to provide security on the monitor node selection process which still remains susceptible to intelligent attacks. The adversary with sufficient hardware and software modules of cryptanalysis technique can easily revoke the secret keys and the original data by sensing the unsecured channel. By finding the locations of sensor nodes, the intelligent attacker can harm the data communication or the node performance [28].

The proposed scheme would provide a suitable solution against these issues by making a secure routing and monitoring mechanism against global adversaries in Ad hoc sensor networks using random node selection approach. This work has the following contribution:

1.Proposes a hybrid routing scheme using two routing protocols: 1. Optimized Link State Multipath Routing (Proactive); and 2. Ad hoc On-demand Multipath Distance Vector Routing (Reactive) discussed in Section 4.2;

2.This is the hybrid routing and monitoring mechanism with an ability to act as proactive (link-state) and reactive (distance-vector) depend on time with the help of Modified Two-Fish algorithm discussed in Section 4.4;

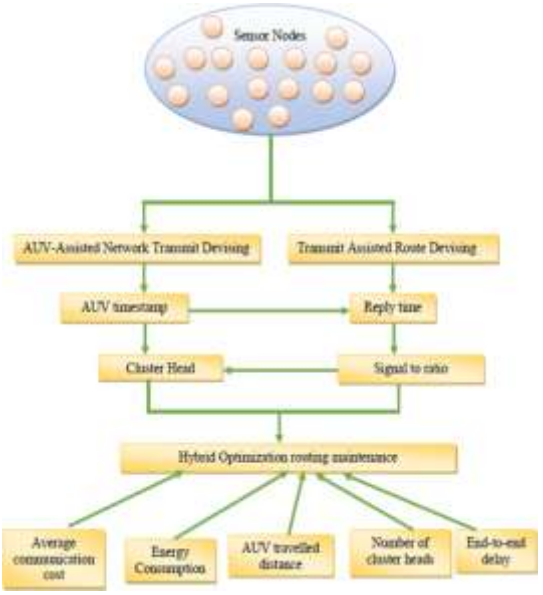
3.It is used to select the optimal paths for data transmission nodes as well as monitor (guard) nodes with the help of several optimization algorithms to attain Concealed Monitor Set (CMS) and secure data transmission Section 4.4 and Section 4.5; and

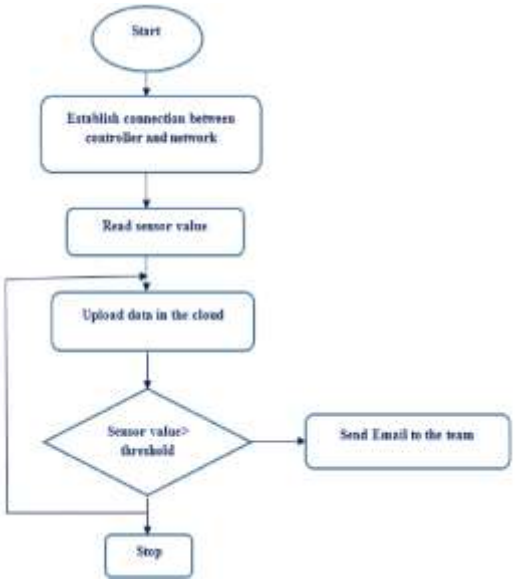
4.This proposed protocol finds the optimal routing paths depending upon the network scenario, nodes mobility, frequent link breaks, consecutive update rate, network functionality, obviously sensor nodes energy levels and so on discussed in Section 4.7.

Generally, the routing protocols are used to find the optimal path between source and destination nodes to transmit the data; but it does not select the monitor nodes in multi-path environments. In the above scope, this hybrid routing and monitoring approaches have been developed and the purpose is to provide better security on the multiple channels. The selection of monitoring nodes is done efficiently at the time of the routing process. By using these combined routing functionalities and sensor monitor selection approaches, the multiple channels are protected using two fish symmetric cryptosystem with unpredictable key shares derivation and the data is transmitted between Ad hoc sensor nodes efficiently; even though the Ad hoc sensor nodes are identified by the multiple global adversaries at the meantime.

The remaining sections of the paper are organized as follows: Section 2 discusses the literature works related to ad hoc routing protocols. Section 3 formulates problem statement, network design, adversary model, routing and monitoring, algorithms and channel-dependent key shares for IoT-based WSNs. Section 4 presents the architecture of the proposed system and routing algorithms. Section 5 demonstrates the simulation results of the proposed system in comparison with other routing protocols. Section 6 concludes the research work.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 5 May 2022, pp: 284-288 www.ijaem.net ISSN: 2395-5252





Related works:

Generally speaking, Wireless Sensor Networks (WSNs') are widely used to provide responsive information in a wide range of applications. Data concealment over the open communication medium is offered to protect the sensor nodes and network data, and thus it has now been picked out randomly or hierarchically for the detection of adversaries. Several routing protocols have been proposed for mobile ad-hoc networks [28]. Each routing protocol has a particular application scenario and

Research background

This section discusses the problem statement, network design, adversary model, routing and monitoring, algorithms and channel-dependent key shares for IoT-based WSNs.

Proposed security architecture

Fig. 3 illustrates the architecture of the proposed system. The sensed real-time environmental factors are converted into a collection of bits bt and transmitted to other sensor nodes with respect to time interval t. In these WSNs, the single or multiple senders may transmit their data to one or more destinations. As understood above this is dense WSN, there are many proactive and reactive routing protocols to select the optimum paths to route the packets.

II. RESULTS AND DISCUSSION

This section provides the details of the simulation of the proposed system. The algorithms are implemented in Network Simulator Version 2.34 [69] with the integration of OTCL (Object Tool Command Language). It is a powerful tool to simulate the mobile ad hoc networks that provide a low-level insightful operation to examine the network topology including sensor nodes, network link, application protocols, and queuing. In this research, the routing protocols are carefully designed to test the

III. CONCLUSION

The proposed hybrid routing and monitoring mechanism have been designed and implemented with dynamically selected sensor monitor nodes in ad hoc sensor networks to improve secure data transmission. To offer flexible security, a secure routing and monitoring protocol was proposed with multi-variant tuples using symmetric key approaches such as MARS, RC6, Serpent and Twofish. This proposed approach discovered and prevented the adversaries in the global sensor network. The proposed approach

Declaration of Competing Interest

None.

B. D. Deebak is presently working as Associate Professor in the department of Computational Intelligence, School of Computer Science and Engineering at Vellore Institute of Technology, Vellore, India. He previously associated with GMR Institute of Technology, Rajam (AP) as Associate Professor in the Department of Computer Science and Engineering. He also associated with Middle East Technical University (METU) Northern

Cyprus Campus during 2016–2017. He has more than 12 Years of Teaching

Research data for this article

Data not available / No data was used for the research described in the article

About research data

REFERENCES

[1]. J.H. Kong et al.**'A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments**J. Netw. Comput. Appl.(Mar. 2015)

[2]. M. Sánchez et al.**ANEJOS: a java based simulator for ad hoc networks** Future Generation Computer Systems (2001)

[3]. B. Farahani et al. **Towards fog-driven IoTeHealth: Promises and challenges of IoT in medicine and healthcare** Future Gener. Comput. Syst. (2018)

[4]. A. Kumari et al. **Fog computing for healthcare 4.0 environment: Opportunities and challenges**

[5]. Comput. Electr. Eng.(2018)

[6]. F. Al-Turjman et al. **Smart Parking in IoT-enabled Cities: A Survey** Elsevier Sustainable Cities and Societies (2019)

[7]. M. Khalaf et al. **New efficient velocity-aware probabilistic route discovery schemes for high mobility Ad Hoc networks** J. Comput. Syst. Sci.(2015)

[8]. A. Bamis et al.**A mobility aware protocol synthesis for efficient routing in ad hoc mobile networks**

[9]. Comput. Netw.(2008)

[10]. F. Al-Turjman **Intelligence and Security in Big 5G-oriented IoNT: An Overview** Elsevier Future Generation Computer Systems(2020)

[11]. S. Agrawal et al.**Survey on anomaly detection using data mining techniques** ProcediaComput. Sci.

[12]. (Jan. 2015)

[13]. I.F. Akyildiz **Wireless sensor networks: A survey** Computer Networks (2002)