Journal of Advances in Science and Technology
Vol. 18, Issue No. 1, March-2021, ISSN 2230-9659

Review on Security Measures for Wireless Sensor Network Assisted Applications

P. Geetha[1]* Dr. Sanjay Kumar[2] Dr. Jambi Ratna Raja Kumar[3]

[1] PhD Student, Kalinga University, Raipur

[2] PhD Guide, Kalinga University, Raipur,

[3] Principal, GSMCOE, Pune

Abstract – Wireless sensor networks (WSN) were utilized in gathering iformation from human body, war fields, smart power grids, and interstate highways. Sensors have hardware, storage, and computational restrictions. Developing effective ways to secure data in sensor networks is difficult. In most secure interactions, clients validation with significant formation were required safety tasks. Authentication of user permit intercommunication companies in verifying its intercommunication client's identities. This shared secret session key protects all exchange information once users have been correctly authenticated. Weaknesses in WSNs include security and privacy, limited computation and energy, and dependability difficulties. Wireless sensor networks are commonly utilised to monitor and transmit data. Concerns about security and privacy have been raised about wireless sensor networks. Attackers may easily obtain access to wireless sensor networks by ifusing mischivous information into them. Wireless sensor network were thought being attack-prone. In covering practical situations and applications, as well as the security challenges related to wireless sensor network. Issue of Wide range with concerns in contemporary uses necessitates much study in this field.

Keywords – Wireless Sensor Networks; Sensors, Security; Privacy; WSN Applications

---------------------------------X--------------------------------

1. INTRODUCTION

Traditional communications require simply two communication units. Merelying on proving and verifying is common in most current user authentication methods [1]. The verifier interacts with prove to confirm his identity. The trend lately is to communicate as a group, or many-to-many. For group communication with numerous users, age old clients validation that allowing a users at a certrain instant becomes unacceptable

It has recently been suggested to utilise group authentication [2] to identify whether all users are part of the same group. As a result, group authentication is incredibly efficient. Because group authentication cannot identify non-members, these could get utilized with before hand processing step before clients validation. Members not belonging need extra one-to-one client authentication. Sensor pairwise shared keys are the most used WSN key establishment mechanism.

WSN connection is not guaranteed by Eschenauer and Gligor's initial random key predistribution technique. Each sensor has a random key preloaded from a huge pool [3]. A secure connection may be established between two sensors that share at least one key. If not, they should find a route with secure linkages between them. The key size on each sensor and the key pool size are determined to ensure communication. A Q-composite system was developed to improve the random key method's durability. Using the node placement information, an upgraded random technique was presented.

Any three sensors may form a triple key between themselves. WSN connection is guaranteed through deterministic protocols. Most deterministic algorithms use threshold cryptography. Most deterministic methods use pair-wise shared keys between sensor pairs. To establish keys using polynomials, we used the first pair-wise threshold cryptography system. In order to construct pair-wise keys for sensor nodes, an asymmetric matrices and a maximum rank distance matrix are used [4].

A new research proposes a multivariate polynomial-based pre-distribution technique for sensor networks. Leur approach has the benefit of limiting sensor storage space linearly based on network size. WSNs have recently suggested and utilised public-key based methods. In this case, the data packets are encrypted using the digital signature crypto method. elliptic curve encryption technique and architecture for safe applications. However, public-key calculations are resource intensive. Data collection in WSNs requires secure end-to-end connectivity. The data must be sent from source sensor to sink sensor [5].

A network of connections transmits collected data. A pairwise shared key is used to safeguard data in all current end-to-end routing systems. It employs hop-to-hop solutions to allow secure data connection between two parties. Because random key pre-distribution does not ensure communication between two sensors, it is not recommended for use in pair wise shared keys. It leverages differentiated key pre-distribution in its end-to-end secure communication strategy. A sensor's durability is improved by giving it varied numbers of keys.

The wireless sensor networks feature several sensor nodes to monitor environmental factors such as noise, temperature and humidity. With wireless sensor network, weather conditions were controlled through geographically scattered sensors. It is then transmitted to the central location. The sensor is controlled via both side-direction regulated network [6.]. In true, such network were designed to serve military purposes. In the medical, educational, and industrial areas. The wireless network consists of thousands of nodes, each with its own sensor [7]. Sensor network components include battery, antenna, transmitter, receiver, and microcontroller. In order to be economically viable, a network must meet some fundamental conditions. The sensor hops employ routing and flooding to propagate data. Area checking sensor networks can identify things in any location. To be used in the therapeutic field, compensators may be injected into the patient. Due to their high security, they may be used outside. It's popular in telemedicine. By using particular sensors, the doctor can monitor the patient's health and illness severity [8]. It has built-in security mechanisms. Information security is critical in this kind of service delivery.

To reduce transmission overhead and energy consumption, WSN base stations must constantly gather data from end users. This is done by grouping the hubs into clusters. Bunching is the division of hubs in a group based on a plan. A sensor array's lifespan has been shown to be improved by bundling [9]. In order to maximise energy efficiency and flexibility, grouping is completed. For the bunch to be developed, the parts must be positioned around the hub. Members Nodes are responsible for detecting and relaying data to the Cluster Head (CH). As with every solution, there are pros and cons. Various sinks of mobile dependent routings methods was developed in providing equilibrium for consumption of energy throughout sensor’s area and minimise averaged end-to-end latency regarding routing sensor information, but many consist of disregarded time-sensing uses.

Network design of wireless 5 horizontal with 3 upright tiers. Communication consumes energy. Inactive, sleep, and active [10] are the three radio channel operating modes. The energy usage may be reduced by shortening the delay between transmitter and receiver [11]. Another technique to save energy is to reduce switching state. Using sensor nodes effectively reduces packet collision [12]. In order to overcome the aforesaid issue, duty cycle is essential. Routing may determine the network's longevity [13]. Wireless sensor networks often suffer from poor service quality difficulties. Based on traversal counts, node, path and QOS was calculated. With such category is the issue of bandwidth [14]. Sensor networks provide the following advantages: dependability, accessibility, and serviceability Considering these limits promotes financial instability. The first layer controls network traffic [15].

Until the user receives favourable information, data conversion continues. It also has several measures to prevent unnecessary congestion. Finally, data link layer controls errors [16]. High powered systems include technological components like battery and radio. Aside from the architectural based assessment method, several devices offer specific functionality. It is simply required contents to conduct the fundamental mechanism for quality of service. The lack of wired networks and scalability are the benefits of wireless communication fields. No cables are used to transmit information. However, it communicates using electromagnetic radiation utilising an antenna. Installing it is easier due to the versatility. Inefficient information exchange on a wireless network may enhance productivity. Roving is possible without losing the contributor-receiver relationship. The sensor network's functioning is determined by the node's size and number. Using a transceiver, introduce electromagnetic waves. This network has several applications in computer networking. This increases the design expense. Compensator networks identify the item availability. Some individuals profit more than others from business, industry, and research. But, enhancing information transfer behaviour regarding effective balancing of load between the node was not successful completely avoiding previously energy LEACH and adaptive conscious clusters dependent routing (AECR) protocol having long Distance dependent Threshold (LEACH-DT) protocol from minimising communication overheads and energy depletion. A protocol called Enhanced Fuzzy C (ECATS) is developed to enhance network communication [17].

2. REVIEW OF WORKS

This section describes the Novel Security Based End-to-End set of rules of Routing for Wireless Sensor Network from a high level. This section highlights current research interests and contributions.

Green TDMA Scheduling Algorithm pertaining to Wireless Sensor Network was introduced by authors in paper [18]. Single information chunk was gathered with single cycles in k-hop WSNs. Our theoretical research determines best k for maximum net work life. This article examines need maximum energy use, timeslots, and leftover energy network . Suggested method is successful with regards to TS scheduling and energy efficiency, as shown by theoretical and numerical analysis and simulation.

A cluster-based routing system for wireless sensor networks was developed by the authors in paper [19] On the basis of network size, AECR protocol clusters scattered sensor nodes. The creation of random clusters is prevented, and CH roles are spread uniformly over the network area. Weighted metrics for CH election reduces computational overheads and energy usage within each cluster zone. This protocol also finds the quickest, most energy efficient, and most reliable multi-hop data transport routes. It also adjusts CH roles according to network circumstances rather than re- clustering them constantly in load distribution equilibrium. Set of rules regarding AECR outperforms previous solutions in several assessment measures.

Trustable Routing and Secured Wireless Sensor Network was suggested by the authors in paper [20]. Based on active detection, we offer a unique security and trust routing strategy with the following great properties: (1) High routing success rate, security, and scalability. So that almost every route is successful, the Active Trust scheme can identify and avoid questionable nodes. (2) Efficient energy use. Active Trust completely utilises residual energy to build numerous detection paths. Our technique increases the likelihood of failproof routing through extra comparatively three folds, and in certain circumstances by ten times, theoretically. Our system also increases network security and energy economy. Wire-less sensor network security is critical.

A Cuckoo Optimization Algorithm for Energy-Aware Clustering-Based Routing in Wireless Sensor Networks was reported by the authors in paper [21]. Wireline sensor networks (WSNs) may be clustered and selected optimally by employing the cuckoo optimization method. With respect to choosing cluster heads, the suggested technique assessed four factors: remaining energy, proximity with base stations, between-cluster distances and within-cluster, and cluster distances. When compared to existing algorithms such as LACH-EP, LEACH, and LEACH with proximity-dependent threshold, suggested technique outperforms them in form of average packet rate of delivery having first node death in six different situations.

A Content-based Mobile Sink's Wireless Multimedia Sensor Network has been explored by the authors in paper [22]. To allow position independent networks with minimal redundancy information aggregations, we present a unique QoE- accronymed content-based networks architecture regarding MS-WMSN. Queries about quality of experience (QoE) force each network node to build an HCNT. The mobile sink selects and stores the sensing data depending on QoE criteria. Calculus model of stochastic network nature is also designed for examining worst-case performance regarding suggested network's example. Proposed paradigm lowers communication time from end-to-end in simulation.

To analyse and cluster big data blocks, the author uses the Enhanced FCM clustering method [23], input data are given to the algorithm, along with a predetermined number of clusters. Each data point is then connected with all possible clusters of B degree. Individual clusters label this degree as B membership. A data point may be in more than one cluster. An iterative splitting of the data set produces clusters. When the goal function is minimised, the procedure stops.

Applying AES (Advanced Encryption Standard) as an encrypted technique in a cableless sensor network was suggested by the authors in paper [24]. For encryption and decryption, both parties utilise the same AES-based symmetric key. With this approach, the encrypted text is generated quickly by doing ten mathematical rounds.

The authors in paper [25] introduces an effective cryptographic solution for WSN data security utilising Latest Encryption Standard Version-II. MES V-II presents a balanced encrypted method. A randomised TTJSA and DJSA algorithm created by Nath and co-workers. This technique uses a modified Verna cypher with variable block sizes and keys. This technique also includes feedback as an extra security requirement for this algorithm. A modified Verna cypher technique with feedback and a fresh key is used after direct stage encryption. Repeating this process creates a very secure system.

Both picture and text encryption may be done by employing chaotic map and genetic processes as described by the authors in paper [26]. Using this method saves energy and reduces computing requirements. A secure route is needed to distribute the started parameters.

The authors in paper [27], the suggested flooding technique adds complexity to the security, making it harder for an opponent to identify the true packets. Its application in big and crucial WSNs is still questionable due to the protocol's limited testing in small networks.

The authors in paper [28] shows that the trust support schema accurately detects malicious nodes with little false positives. However, it only considers attacks on the packet; many other sorts of attacks were not evaluated.

The authors in paper [29], the author discussed sensor node monitoring, tamper-proofing, detection methods, hash function, mobile-agent based, reactive, spread spectrum, defensive protocols, duty cycle, priority message, cryptographic algorithms, region mapping among others.

The authors in paper [30] suggested Algorithms give dependability while protocols provide congestion management. Reliability ensures that missing data chunks were recognised and again sent unless they are rececieved at destined location. Transport layer threats include de-synchronization and flooding.

The authors in paper [31] suggested sensor nodes adopt sleep mode to save energy and extend longevity. Sleep-Denial attacks or torture of sleep deprivations tortures studied. 3 methods exixt to combat sleep deprivation. Primarily and most important approach is robust data-link-layer authentication. The implementation uses the IEEE 802.15.4-based Tiny OS and Tiny SEC authentication techniques. The second approach is anti-reply protection, such as the CARP protocol. A denial-of-sleep attack may be captured by broadcasting attack protection. The Zero Knowledge Protocol (ZKP) being newest protocol pertaining to denial-of-sleep attacks.

3. SCENARIOS of APPLICATION

Utilization of Wireless sensor network deals with critically sensitive information having essential data, making them crucial system. Wireless sensor networks were commonly utilised in exchanging data between nodes. It has been a decade since sensor network technology has advanced to the point where diverse applications have emerged. Three applications are examined for the practical research ideology.

4. SECURITY VULNERABILITIES, ISSUES, AND ATTACK ANALYSIS

A wireless sensor network's security is critical. A few conditions must be met for wireless sensor networks to be secure. These prerequisites apply to all three motivating applications.

(1) Secure authorisation is important because only approved sensor nodes must be capable in accessing networks.

(2) A network's message and node identities must be verified. Attackers should be unable to fabricate data that is indistinguishable from benign data.

(3) Network-related meta-data must be hidden from everyone, including network administrators.

(4) Information and Data held within node's memory like flash must not get disclosed in front of attackers or unauthorised people under any circumstances.

(5) Securtiy and privacy regarding information within networks should never get compromised. Personal data of elderly persons are included in the aforesaid small-scale motivational application, and such data must be protected.

(6) The sensor network services must be always accessible and not susceptible to DoS attacks. A service's availability in the network amid system failures and malfunctions is also critical.

(7) Resistance against DoS attacks is essential. Because all three incentive apps are susceptible for DoS attacks.

(8) New incomming messages should gets validated in every application during data exchange to prevent the attacker from reusing earlier data.

(9) The protocol must resist node compromise attempts. Applications on a small scale are subject to node compromise attacks

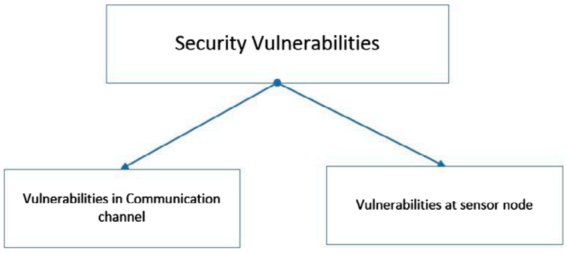
Security Vulnerabilities
Vulnerabilities in Communication channel
Vulnerabilities at sensor node

Figure 1. Wireless sensor network's security attacks Classification.

Latest upcoming wireless sensor network communicate via electromagnetic waves amongst sinks and sensor nodes. To build an ad-hoc multi-hop radio network, WSN sensor nodes communicate. Multiple security flaws exist in wireless sensor networks now. As indicated in Figure 1, we research and categorise threats. Communication channel vulnerabilities are most common between two sensor nodes. While the intruder does not need access physically partaining to nodes of sensors, other network equipments, malicious data may be put into them to cause havoc. Eavesdropping may occur in attacks on confidentiality and privacy. The contents of a network may be discovered when end-to-end security fails. An attacker can do this by listening in on the network's frequency. It is feasible to use this kind of attack on the previously described small and medium sized apps. A person's health information related to heart rate, activities, and movements might be acquired by an attacker if networks of sensor implemented within assisting living facility regarding elderly are eavesdropped.

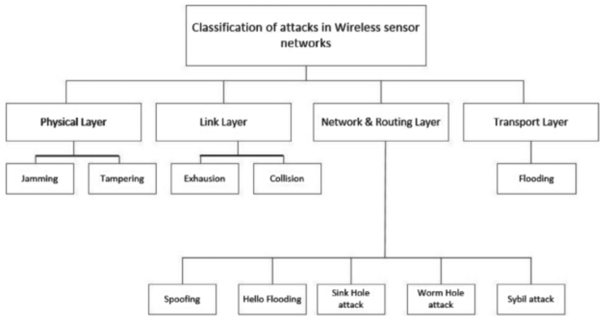

Figure 2. Classification of vulnerabilities

Physical layer attacks target sensor node vulnerabilities. Attacks against wireless sensor nodes include manipulation and node capture. If an attacker has access to a sensor node in a network, they may do the following [28]:

- Theft of data (Sensitive data).
- Changing the default behaviour of the nodes.
- Physically harm senor nodes and disable their services.

Memory security is a problem for node security. Every sensor node in contemporary wireless sensor network has modest quantity of flashs memories to store temporary data. Temp memory size varies from small to big programmes. In big applications like environmental monitoring, information transferred to base station with fixed gaps of time, but is retained on sensors node for time period. Medium- and small-scale applications would also retain data on sensor nodes for a limited duration. The attacker may modify the crucial before transmission if they had access to this memory. A temperature record maintained in the memory for a period of time might be manipulated by an attacker gaining access to the specific node, causing fake emergency in that area. Figure 2 classifies security threats on wireless sensor networks. We characterise attacks using wireless sensor networks. Other attacks may exist, but the motivated application vulnerabilities are evaluated in this context.

5. CONCLUSION

Modern wireless sensor networks are not contained. Wireless sensor networks were vulnerable to attacks because of their nature. These programmes are used to reveal security flaws in this research. This research examines wireless sensor network security from diverse networks. Wireless sensor network were employed within missions critically uses, according to study results. However, protection risks with wireless sensor network were substantial.

This research analysed available fixes for security compromise in depth. With respect to this concept, cryptographic algorithms research with sensing of intrusion systems is fully examined. Intrusion detection systems (IDS) identify potential attackers, while cryptography techniques help prevent attacks from occurring. So we need a good cryptography system for this reason. Because wireless sensor network is resources restricted, techniques must get viable, best adjusted in delivering excellent safety having little resources in use.

Consideration is given to the application situations, and suggestions are made as to which solution is most appropriate for each. This two-phase hybrid cryptographic algorithm (THCA) is anticipated for big and medium-sized applications, as shown in the comparative table. Because THCA requires a lot of resources, it is advised for modest applications. While these methods work within the constraints of the present approaches, additional study is required to optimise and overcome these constraints.

REFERENCES

1. Elhoseny, Mohamed, and Aboul Ella Hassanien. "Secure data transmission in WSN: an overview." *Dynamic wireless sensor networks* (2019): pp. 115-143.

2. Wu, Fan, et al. "A novel three-factor authentication protocol for wireless sensor networks with IoT notion." *IEEE Systems Journal* 15.1 (2020): pp. 1120-1129.

3. Dewal, Prachi, et al. "Security attacks in wireless sensor networks: A survey." *Cyber Security*. Springer, Singapore, 2018. pp. 47-58.

4. Haque, Khandaker Foysal, K. Habibul Kabir, and Ahmed Abdelgawad. "Advancement of routing protocols and applications of underwater wireless sensor network (UWSN)—a survey." *Journal of Sensor and Actuator Networks* 9.2 (2020): pp. 19.

5. Pundir, Sumit, et al. "Intrusion detection protocols in wireless sensor networks integrated to internet of things deployment: survey and future challenges." *IEEE Access* 8 (2019): pp. 3343-3363.

6. Anwar, Raja Waseem, et al. "BTEM: Belief based trust evaluation mechanism for wireless sensor networks." *Future*

generation computer systems 96 (2019): pp. 605-616.

7. Gogolák, László, and Igor Fürstner. "Wireless sensor network aided assembly line monitoring according to expectations of industry 4.0." *Applied Sciences* 11.1 (2020): pp. 25.

8. Fahmy, Hossam Mahmoud Ahmad. *Concepts, applications, experimentation and analysis of wireless sensor networks*. Springer Nature, 2020.

9. Xie, Haomeng, et al. "Data collection for security measurement in wireless sensor networks: A survey." *IEEE Internet of Things Journal* 6.2 (2018): pp. 2205-2224.

10. Kashyap, Ramgopal. "Applications of wireless sensor networks in healthcare." *IoT and WSN applications for modern agricultural advancements: Emerging research and opportunities*. IGI Global, 2020. 8-40.

11. Singh, Pradeep Kumar, et al., eds. *Handbook of wireless sensor networks: issues and challenges in current Scenario's*. Vol. 1132. Berlin/Heidelberg, Germany: Springer, 2020.

12. Bhushan, Bharat, and Gadadhar Sahoo. "Requirements, protocols, and security challenges in wireless sensor networks: An industrial perspective." *Handbook of computer networks and cyber security*. Springer, Cham, 2020. pp. 683-713.

13. Liu, Xingcheng, et al. "A range-based secure localization algorithm for wireless sensor networks." *IEEE Sensors Journal* 19.2 (2018): pp. 785-796.

14. Kandris, Dionisis, et al. "Applications of wireless sensor networks: an up-to-date survey." *Applied System Innovation* 3.1 (2020):

15. Radhappa, Harish, et al. "Practical overview of security issues in wireless sensor network applications." *International journal of computers and applications* 40.4 (2018): pp. 202-213.

16. Osanaiye, Opeyemi A., Attahiru S. Alfa, and Gerhard P. Hancke. "Denial of service defence for resource availability in wireless sensor networks." *IEEE Access* 6 (2018): pp. 6975-7004.

17. Haseeb, Khalid, et al. "Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things." *Ieee Access* 7 (2019): 185496-185505.

18. Dong, Shi, Xin-gang Zhang, and Wen-gang Zhou. "A security localization algorithm based on DV-hop against sybil attack in wireless sensor networks." *Journal of Electrical Engineering & Technology* 15.2 (2020): pp. 919-926.

19. Yang, Guang, Lie Dai, and Zhiqiang Wei. "Challenges, threats, security issues and new trends of underwater wireless sensor networks." *Sensors* 18.11 (2018): pp. 3907.

20. Mishra, Dheerendra, et al. "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks." *Multimedia Tools and Applications* 77.14 (2018): pp. 18295-18325.

21. Yang, Guang, et al. "Challenges and security issues in underwater wireless sensor networks." *Procedia Computer Science* 147 (2019): pp. 210-216.

22. Tan, Xiaopeng, et al. "Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm." *Sensors* 19.1 (2019): pp. 203.

23. Gayathri, N. B., et al. "Efficient and secure pairing-free certificateless aggregate signature scheme for healthcare wireless medical sensor networks." *IEEE Internet of Things Journal* 6.5 (2019): 9064-9075.

24. Dhivyasri, K., A. Suphalakshmi, and M. Revathi. "Wireless sensor network jammer attack: A detailed review." *Int. J. Res. Appl. Sci. Eng* 8 (2020).

25. Zhu, Jinghua. "Wireless sensor network technology based on security trust evaluation model." *International Journal of Online Engineering* 14.4 (2018).

26. Zhang, Ping, et al. "A secure data collection scheme based on compressive sensing in wireless sensor networks." *Ad Hoc Networks* 70 (2018): pp. 73-84.

27. Shi, Qiong, et al. "Information-aware secure routing in wireless sensor networks." *Sensors* 20.1 (2019): pp. 165.

28. Kumar, K. Vinoth, et al. "SDARP: Security based Data Aware Routing Protocol for ad hoc sensor networks." *International Journal of Intelligent Networks* 1 (2020): pp. 36-42.

29. Vinodha, D., and E. A. Mary Anita. "Secure data aggregation techniques for wireless

sensor networks: a review." *Archives of Computational Methods in Engineering* 26.4 (2019): pp. 1007-1027.

30. Tang, Jiawei, et al. "A trust-based secure routing scheme using the traceback approach for energy-harvesting wireless sensor networks." *Sensors* 18.3 (2018): pp. 751.

31. Guimaraes, Raniere Rocha, et al. "Intelligent network security monitoring based on optimum-path forest clustering." *Ieee Network* 33.2 (2018): pp. 126-131.

Corresponding Author

P. Geetha*

PhD Student, Kalinga University, Raipur