JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

WIRELESS SENSOR NETWORK SECURITY AND ITS APPLICATIONS

Maitri Rashmikant Sakarvadia
Research Scholar at Sabarmati University (Formerly, Calorx Teachers' University), Ahmadabad, Gujarat, India

ABSTRACT

Due in large part to the support provided by the internet of things, "wireless sensor networks" are now making tremendous ground in their development. "Wireless sensor networks" have the capacity to instantly send any essential data to people who need it, regardless of where they are located or how much time has passed since the data was collected. The rise of the Internet of Things is supported by a strong basis that is supplied by the extensive use of "wireless sensor networks". This foundation is provided by widespread usage of "wireless sensor networks". It is very necessary to do research on the security of "wireless sensor networks" in order to cut down on the chance of the network being subjected to assaults and security breaches. This is essential due to the fact that the node deployment environment of such networks is often one that has a high level of sophistication. The benefits of "wireless sensor networks", including how secure they are and how helpful they may be, are the primary subject of this essay.

KEYWORDS: Application of WSN, Wireless sensor network, Communication, Security of WSN..

INTRODUCTION

Sensor is principal instrument for sensing information in a "Wireless Sensor Network (WSN)". Use of sensors for purpose of the environmental sensing and the subsequent data transmission through wireless networks contributes to an improved ability to meet the requirements of end users. Any compromise in security might potentially have disastrous repercussions due to the "high technical content and complex structure" that "wireless sensor networks" depend on. The development of "wireless sensor networks" has facilitated both the acceleration of interpersonal communication and the expansion of the "Internet of Things (IoT)". [1]

Because it's having such a broad variety of applications, WSN may be used to gather any sort of data or information and to handle any complexity in any environment. This is made possible by its adaptability. The detection of biological and chemical contaminants in addition to radioactive radiation, as well as the detection of troop deployments in enemy territory and other situations, is only some of the military uses that this technology has.

It may be used for variety that spans purposes at environmental protection & monitoring, such as data collection from field, the tracking of animal footprints, the examination of pollutants, and the forecasting of explosions caused by forest fires and debris flows. Monitoring the growth of the crop and tracking the flow of products is an essential component of intelligent production in both the industrial and agricultural spheres. It is possible for it to carry out the medically beneficial responsibilities of collecting and evaluating the physiological data of patients and giving rapid medical treatment to such patients. The "smart home," "smart transit," "smart city," the preservation of cultural relics and commerce, to name just a few examples, are just a few of the domains in which "wireless sensor networks" have shown to be quite useful. The introduction of the WSN is causing a paradigm shift in society [2].

Information security for WSNs is a concern in a wide variety of contexts, including the healthcare industry, the military, and disaster relief efforts. If proper security protection measures are not in place, data that is sent across "wireless sensor networks" is very vulnerable to attacks from both the inside and the outside [3]. WSN networks, on the other hand, are unable of handling the enormous quantities of processing that are necessary for cryptographic defensive measures. Consequently, selecting an appropriate encryption scheme to safeguard WSN data is a difficult and time-consuming task [4].

WSN'S CHARACTERISTICS:

The features of "wireless sensor networks" are as follows:

Organizational liberty

The design of the sensor that is used for the wireless network is free from any restrictions. An organizer is able to simply build a fully working "wireless sensor network" at any time or location, and all future administration and maintenance responsibilities may be done centrally [5].

Topology Uncertainty in Networks

When viewed in light of the network's organizational structure, the design of the "wireless sensor network" might undergo changes. It is possible, for instance, to change both the total number of sensor nodes that are used to construct the network topology and the order in which these nodes are shown on the topology diagram.

There is no centralized control

In spite of the fact that "wireless sensor networks (WSNs)" have "centralized control of base stations & sensor nodes", For each host-independent operation, the network of terminals between sensor nodes will govern the mode of control, the routing, and the host's function, the fact that WSNs do not interfere with each other makes them very resilient and difficult to destroy [6].

The level of safety is low

Because they communicate information wirelessly with one another, the sensor nodes that make up a "wireless sensor network" are susceptible to interference from the outside world. As a direct consequence of this, the majority of the nodes that make up the WSN are not protected from interference from the outside, which significantly reduces the level of safety afforded by the network [7].

PROTECTION OF WSNS

Security for "wireless sensor networks (WSN)" is a field of research that is advancing quickly. Because of the way they are designed, "wireless sensor networks" are open to a wide variety of threats, which puts the data security at risk in a variety of settings. It is not possible to transport the data obtained by the sensor node to the designated sink node in a timely and correct way, particularly when an attack is made on the routing of the network. As is the case with more traditional computer communication networks, security of information kept in "wireless sensor networks" may be compromised by a wide variety of malicious intrusion techniques. Because of the "radio characteristics of wireless channels" & the properties of "ad hoc networks", which make passive assaults and active attacks more viable, "wireless sensor networks" have a high risk of being attacked by a denial-of-service [8]. This is the case owing to "radio characteristics of wireless channels". "Sensor networks" are going to be monitored, tampered with, forged, and blocked by attackers. The following is a list of instances of attacks that may be carried out against "wireless sensor networks":

- Threats to a network's physical layer assaults that cause congestion & to physical damage. If a potential victim is aware of "wireless sensor network's communication frequency", they may launch a congestion attack. An attacker using this tactic will often radiate radio noise around the network's central frequency. The network will stop working properly as a result of this. Sensor nodes are physically vulnerable since they are often deployed in unmonitored areas, and it is easy for adversaries to gain control of sensor nodes and disguise them inside the network in order to eavesdrop on or damage the system.
- Attacks based on collision, weariness, and unfair competition may all potentially cause the connection layer to become more vulnerable. Collision attack is a situation in which an adversary sends a cluster of malicious data to a genuine node, which causes the output signals to mix together and make them unreadable. The phrase "collision attack" refers to this kind of scenario.
- The network layer is responsible for many different things, including but not limited to direction misdirection, sink hole attacks, sink node attacks, discard and selective forwarding, and many more. When an adversarial node is present in a network, that node may choose to ignore all or a portion of the data packets it gets from an upstream node, or it may deliver those data packets selectively. Rogue nodes may combine their data into bundles and send them with a high delivery priority in order to disrupt the normal flow of communication throughout the network. Both flood assaults and synchronized damage attacks are considered to be within the transport layer's purview. In a flood attack, the attacker makes several attempts

to get to know one another a nearby "sensor node", ultimately depleting that node's capacity to do so and perhaps compelling it to reject other requests that are legitimate in nature.

- An attacker may use direction misdirection, also known as a false routing information attack, intent on accomplishing their goals of splintering network & rising latency at both ends. In this attack, the attacker forges, tampers with, or replays routing information in order to loop the network's routing, draw or repel traffic, lengthen or shorten the route to its origin, and so on.

When attempting to characterize security function of "wireless sensor networks", it is helpful to integrate an examination of potential threats to the network on all levels with characteristics of the networks themselves. Theft of data and listening in on conversations may be prevented by using a system that has both robust encryption and a dependable key management mechanism. Maintaining the integrity of the data to prevent illegal modifications to the records; The data must be up to date in order to prevent malicious nodes from overwhelming the network with unnecessary queries; The ability to see and record the actions of users while they are logged into the system; Because of non-repudiation, none of the sensors in the network will be able to dispute that their activities took place; control of authorization and access, together with encryption and mutual authentication of network nodes functioning in the capacity as sensors; Because the hardware is safe, there is no possibility of any sensor nodes being stolen or broken into [9].

WSN security confronts additional issues that are not encountered in standard wireless networks [10], due to most sensor nodes being embedded in buildings located in an area that is not secured and that these nodes have limited energy, data processing, storage, and communication capacity. This demonstrates that the typical precautions used to secure wireless networks are not adequate to guarantee the reliability of WSNs.

Critical Technology

Optimization software for node security

The use of technology that enhances the level of security at individual nodes may also be utilized to fortify the defenses of "wireless sensor networks".

In this research, we provide a solution for optimizing node security based on a "ternary key distribution scheme". This technology has potential to streamline the topologies of "wireless sensor network" systems and increase their resistance to assaults [14]. During the optimization process, the nodes of the "wireless sensor network" should ideally be clustered together. This will enable the optimization to be performed using safe routing and key computation, which is important for maintaining network security. Each cluster's key is distributed in one of three ways based on the cluster's individual requirements for key computation and security, and the entire network works together to fine-tune its adaptive security routing [11]. The "topology of a wireless sensor network" is comprised of many sorts of nodes.

When there is a rise in the signal's strength, the coverage area provided by the cluster heads grows to suit it. The values of a random number generated by a wireless sensor node are compared to a predefined threshold value in order to identify which nodes will serve as cluster heads. A node that belongs to the cluster head may be recognized by reducing the range over which the threshold operates [12].

The calculation of a key must conform to one of three unique forms in order for any one of the three techniques of key distribution to be put into practice. The three most significant connections are the one between the connections between the "base station & the cluster head, cluster head & the sensor node, & the sensor node & base station". Encryption of data sent through "base station nodes" should employ the Kn key. It is possible that "sensor node & base station" will have to do some very important computations together to be satisfied. After getting announcement from "base station", "ordinary sensor nodes" are required to use Ks in order to decode the data included within the broadcast message. You will, at some point, be forced to evolve and adjust. The combined data should then be sent to the command and control center so that exact adaptive modifications may be performed. For instance, wireless networks only have a single, oversimplified degree of clustering to choose from. In order to provide the highest possible level of safety, it is necessary to perfect and perfect both the "base station routing algorithm & sensor node routing algorithm" [13].

Whether or not "base station" is required for message broadcasting is a key factor in optimizing the routing algorithm used by "base station". Message must be encrypted using key 'Kn' before it can be sent through the base station. "Cluster-head node" may be identified automatically if broadcasting is not required. Check to see whether the data was successfully transmitted. If the data that was transmitted is located, then using the node ID and the key KS, it may be immediately decrypted. Incomplete or incorrect data packets must be thrown out during the MAC verification procedure; if not, the raw data must be processed before the desired results may be obtained. Using a Kn key, the data is encrypted before being sent to the cluster head as part of an adaptively adjusted routing mechanism for sensor nodes. Decryption of individual packets is possible using Kc; the cluster head then appends its own ID to the mix before sending 'Kn' - encrypted data to "base station" [14].

FUSION TECHNIQUE FOR DATA SECURITY

Data fusion inside a "wireless sensor network" makes it easy to fight a range of security risks. This is made possible by the fact that nodes of "wireless sensor networks" are often located in settings that are neither monitored nor particularly secure. It's crucial to supply a complete security system to ensure safety of one's data in light of the declining cost of electricity. Techniques for data integration such as data rolling and data integrity algorithms are becoming more used in today's "wireless sensor networks". The second one is based on privacy of data, whereas first one is based at integrity of data. In addition, encryption techniques make use of additional symmetric cipher algorithms of the data fusion approach in order to guarantee the confidentiality of the data. These strategies have a high applicability to advantage; nevertheless, there is a scarcity of costly aggregation sites. Adjustments may be

made to intermediate nodes during data transmission so that the data does not need to be decrypted. Additionally, via the use of aggregation numbers, the nodes will receive data packets and then transfer their own encrypted data to the parent node. Because of this, less energy will be needed to run activities by existing system. By skipping the decrypted and encrypted connection again, it is possible to drastically cut down on energy usage while still maintaining the integrity of the network. [15] The data security fusion approach is an innovative method of protection that consumes less energy while maintaining a high level of safety.

To guarantee that "data fusion technology" can more effectively protect "wireless sensor networks", it is imperative that a trust-based system for protecting combined data be established. This scheme should include both "direct trust component & element of mutual trust. After the monitoring node module has observed the activity of the network and carried out any necessary pretreatment and calculations, the trust values for the entire CT may be computed using the DT values provided for direct trust, & fusion processing can be carried out based on the outcomes of those calculations. During the course of the fusion process, the cluster nodes need to keep a close check on the fusion nodes that have been sampled and determine whether or not they can be trusted based on how they act.

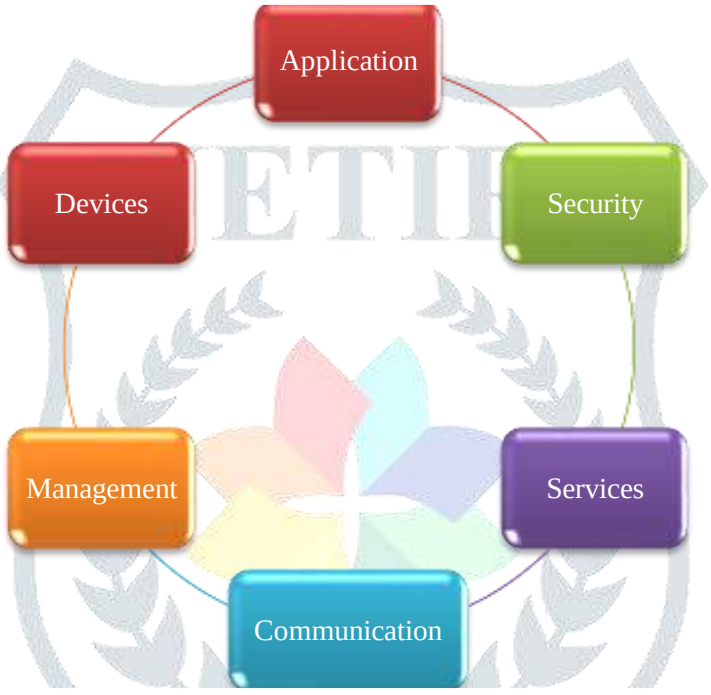
After "result set nodes" have been calculated & examined in combination with "data fusion byte points", it is duty of the "base station" to make ultimate decision. The importance of trust and existing trust DT to arrive to this outcome, the NT history value synthesis technique employs a weighted sum of each "node's direct CT, indirect T, and direct DT trust values". It is recommended to combine all three values after computing each "node's direct trust value DT, indirect trust value CT" & weighted factor. [16]

It is crucial to evaluate whether or not the weighted factor is used, as well as the influence of the periodic behavior features of the trust mechanism & recommended degree of historical trust in fixed node trust, in order to avoid making an error in the calculation of indirect trust. This may be done by thinking about whether or not the weighted factor is utilized. Any comprehensive data fusion security solution needs to incorporate, as part of its architecture, careful consideration of the need to protect individuals' private information. When it comes to protecting the secrecy of "wireless sensor networks", it is common practice to use data fusion protection techniques and encryption processing methods. Based on the findings of this research, it is recommended that a modified version of the SMART approach be used. In order to offer a superior level of service in the area of "wireless sensor network security", the startup of network should begin by establishing the relief valve, and then it should prioritize the transmission of data and the fusion of data. This is due to the fact that conventional SMART systems, which divide data detection, segmentation, and convergence into three steps, have reached a price point that makes them unaffordable. Data transmission must assign unique transmission times to each set of nodes in order to guarantee confidentiality of sensitive data & avoid the inadvertent exposure of the location of the data. Due to the fact that this is not the case, the packet will be stored at the intermediate node I for a period of time T that is completely random before it is transmitted. The foundation of data fusion is the process of extending the data fusion tree, and the key is used in both the encryption & decryption processes [17].

APPLICATION RANGE

Security is a major concern because it affects the connection between "devices (sensor nodes) & applications (cloud computing, business intelligence layer)". However, security is not only enforced at the topmost levels, but also at each successive layer working its way up (fig.1).

Figure 1. Security application



Wireless Sensor Applications in Electrical Automation

As the technology behind automation evolves, it becomes simpler to automate power systems. This, in turn, helps to reduce the amount of wasted energy, avoid accidents, and speed up maintenance and repairs when they do occur. For effective management of a power system, which requires round-the-clock monitoring, a high fault tolerance rate must be maintained at all times. Make adjustments to the voltage depending on conditions from the outside, such as the weather. It is possible that changes in the surrounding environment will have a substantial effect on the characteristics of the power system. The gathering of data is an extremely important part. In order to accurately measure and analyze the values of electrical properties in an electrical network, specialized devices are necessary. Controlling it in accordance with the data that it provides will allow you to give it a higher level of automation. In addition, the majority of wireless sensor devices are used in electrical automation, which helps to avoid specific circuit troubles and boosts the effectiveness of sensor devices. When it comes to the management and

maintenance of a high voltage transmission line for a power system, complexity is the enemy. Complicated lines are more likely to cause accidents. The data that is sent via wireless sensors is superior in terms of reliability and precision [18].

Using Wireless Sensors for Monitoring Applications

The monitoring tools that are put to use during the process of monitoring carried out with the assistance of wireless sensor technology change according to the nature of the monitoring task that is being carried out. Temperature sensing technology is the kind of sensing technology that is applied in the production process more often than any other form. When it comes to the monitoring of industrial production, sensing technology is primarily focused on keeping a close check on the boiler to ensure that it remains in a secure condition. Steel tubes, which are great for dispersing heat, are often used in the construction of water cooling tubes in contemporary boilers. This is due to the fact that heat is created during the process of heat extraction by the boiler. The management of modern boilers makes use of remote computer control to shield personnel from the intense heat created by the cooling process. The remote control system has a high price tag, but in order to use it, the boiler has to be monitored when it is set to a high temperature. During the process of transmitting the data, it is possible to do a direct transfer of measurement data. Because of the increased monitoring and control, the total number of faulty components that are manufactured will decrease, which will lead to a reduction in the cost of production. The employment of "wireless sensor networks" enables a more in-depth monitoring of a number of different components, which eventually results in a product of greater quality [19].

The Use of Wireless Sensors for Location-Tracking

Accurate location and user satisfaction are both within reach with network location technologies. The widespread use of Global Positioning System (GPS) for location services is a reflection of the interactive nature of network data. The method provides pinpoint location pinpointing. A "wireless sensor network" has the potential for precise placement, cheap application costs, and extensive user satisfaction. Both range-based localization and non-distance location are used by WSNs to lock the target's position, although each has its benefits and drawbacks. The former is expensive but provides precise location; whereas the latter is inexpensive but provides inaccurate results. The implications for automobile navigation are enormous. Additionally, certain carryon goods, the real-time whereabouts of some aged or young, and avoiding some susceptible in accidents [20] may all benefit from the deployment of wireless sensor technology.

CONCLUSION

There will be a greater depth and breadth to the use of "wireless sensor networks" as the technologies that control sensors and allow communication continue to grow at a rapid rate. [Case in point:] the Internet of Things. The maintenance of secret keys is expected to get a higher amount of attention moving ahead as the role of providing security becomes more critical. With its scalability, ease of computation, low cost of storage, light

communication burden, and adaptable topology & a host of other WSN attributes must all be taken into account by the protocol and system that is used to manage secret keys. The ability of an application to support a growing number of users is known as scalability. In the subsequent phase of our research, we will investigate how to improve already established strategies and protocols for the management of secret keys. Specifically, we will investigate how to make these strategies and protocols more fault tolerant, self-organizing, and integrated with geographical data.

REFERENCES

1. Meena,O.P. and Somkuwar,A. Comparative Analysis of Information Fusion Techniques for Cooperative Spectrum Sensing in Cognitive Radio Networks.Proceedings of International Conference on Recent Trends in Information,Telecommunication and Computing ,ITC(2014)
2. Prema, G. and Narmatha, D.Performance of Energy a Ware Cooperative Spectruim Sensing Algorithm in Cognitive Wireless Sensor Network.Online International Conference on Green Engineering and Technologies (IC-GET), Coimbatore, 19 November (2016) .
3. Gharaei,N.,Abu Bakar,K.,Mohd Hashim,S.Z., Hosseingholi Pourasl,A.,Siraj,Mand Darwish,T. An Energy-Efficient Mobile Sink-Based Unequal Clustering Mechanism for WSNs.Sensors(Basel),17,1858(2017).
4. Akyildiz, I.F.,Lo,B.F. and Balakrishnan,R. Cooperative Spectrum Sensing in Cognitive Radio Networks:A Survey.Physical Communication ,44,40-62(2011).
5. Alhumud, H.and Zohdy,M. Managing Energy Consumption of Wireless Sensors Networks in Multiple Greenhouses.Wireless Engineering and Technology ,99, 11-19(2018).
6. Wang,N.,Huang,Y. and Liu,W.A Fuzzy-Based Transport Protocol for Mobile Ad Hoc Networks. IEEE International Conference on Sensor Networks,Ubiquitous,and Trustworthy Computing , Taichung, 11-13 June 2008, 320-325 .
7. Zeng,B.and Yan,D.An Energy Efficient Harmony Search Based Routing Algorithm for Small-Scale Wireless Sensor Networks.IEEE 17 th International Conference on Computational Science and Engineering , Chengdu, 19-21 December 2014, 362-367.
8. Lee, H.M.,et al.Optimal Cost Design of Water Distribution Networks using a Decomposition Approach. Engineering Optimization , 48, 2141- 2156 (2016).
9. Hoang, D.C., et al.Real-Time Implementation of a Harmony Search Algorithm Based Clustering Protocol for Energy-Efficient Wireless Sensor Networks.IEEE Transactions on Industrial Informatics,10,774-783 (2014).
10. Parenreng, J.M. and A. Kitagawa, A Model of Security Adaptation for Limited Resources in Wireless Sensor Network. Journal of Computer and Communications, 2017. 05(03): p. 10-23.
11. Vijayarajeswari, R., A. Rajivkannan and J. Santhosh, A Simple Steganography Algorithm Based on Lossless Compression Technique in WSN. Circuits and Systems, 2016. 07(08): p. 1341-1351.

12. Saravanaselvan, A. and B. Paramasivan, Implementation of an Efficient Light Weight Security Algorithm for Energy-Constrained Wireless Sensor Nodes. Circuits and Systems, 2016. 07(09): p. 2234-2241.
13. Savoine, M.M., M.O.D. Menezes and D.A.D. Andrade, Proposal of a Methodology for the Assessment of Security Levels of IoT Wireless Sensor Networks in Nuclear Environments. World Journal of Nuclear Science and Technology, 2018. 08(02): p. 78-85.
14. Liu, Y. and Y. Morgan, Security Analysis of Subspace Network Coding. Journal of Information Security, 2018. 09(01): p. 85-94.
15. Parmar, K. and D.C. Jinwala, Symmetric-Key Based Homomorphic Primitives for End-to-End Secure Data Aggregation in Wireless Sensor Networks. Journal of Information Security, 2015. 06(01): p. 38-50.
16. Mawlood Hussein, S., J.A. López Ramos and J.A. Álvarez Bermejo, Distributed Key Management to Secure IoT Wireless Sensor Networks in Smart-Agro. Sensors, 2020. 20(8): p. 2242.
17. Adil, M., et al., An Anonymous Channel Categorization Scheme of Edge Nodes to Detect Jamming Attacks in Wireless Sensor Networks. Sensors (Basel), 2020. 20(8).
18. Han, D., Du X and Y. Lu, Trustworthiness and a Zero Leakage OTMP-P2L Scheme Based on NP Problems for Edge Security Access. Sensors (Basel), 2020. 20(8).
19. Shang, X., et al., Secrecy Performance Analysis of Wireless Powered Sensor Networks Under Saturation Nonlinear Energy Harvesting and Activation Threshold. Sensors (Basel), 2020. 20(6).
20. Wang, R., Wang, B., Ding, X. et al. Planar array with bidirectional elements for tunnel environments. Sci Rep 7, 15421 (2017). https://doi.org/10.1038/s41598-017-15817-4.