Evaluation of Security Aspects of Wireless Sensor Networks

Niveditha Minnoor
Department of Electronics and Communication
R V College of Engineering
Bangalore, India
nivedithaminnoor@gmail.com

Pannaga Shree B S
Department of Electronics and Communication
R V College of Engineering
Bangalore, India
pannaga.bs@gmail.com

Sahana B
Department of Electronics and Communication
R V College of Engineering
Bangalore, India
sahanab@rvce.edu.in

2021 IEEE International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS) | 978-1-6654-0610-9/21/$31.00 ©2021 IEEE | DOI: 10.1109/CSITSS54238.2021.9683462

***Abstract*— Wireless Sensor Networks require multiple robust security policy implementations in place to effectively secure any data that is being transmitted from or received by it. This in turn, requires efficient security policies and methods designed such that in the case of any attack, data is always protected. A single policy, while being efficient by itself, will not secure the network to the required extent against all types of attacks. Multiple security methods must be implemented in a layered manner in order to provide robust security. In this paper, broad categories of applications of Wireless Sensor Networks, and a brief description of these applications with a focus on security critical use cases such as the military are studied. Security goals and types of attacks with the corresponding countermeasures are evaluated. Various existing implementations of Wireless Sensor Network security protocols are reviewed, and the drawbacks of these methods are discussed. Proposals to overcome these drawbacks are suggested in the final sections of the paper.**

Keywords*— *wireless sensor networks, security protocols, authentication, active attacks, ActiveTrust

I. Introduction

Wireless Sensor Networks (WSNs) collect data from the surrounding environment using a set of spatially dispersed sensors that gather data by measuring, monitoring and recording physical conditions as parameters such as temperature, sound, pollutant levels, humidity, etc. Data measured by these sensors are organized centrally. The wireless transportation of this sensor data requires spontaneous network formation as well as a wireless connection. The initial motivation for these wireless sensor networks was for military applications like battlefield surveillance. The use of these sensor networks has now diversified into consumer and industrial applications, where they are now widely used. Each sensor in the network is called a node. The number of nodes in a WSN can vary from a few hundreds to a few thousands, depending on the requirement of the application. Every node in the network is connected to one, sometimes more than one, central node(s). Fig. 1 is a representation of a typical WSN.

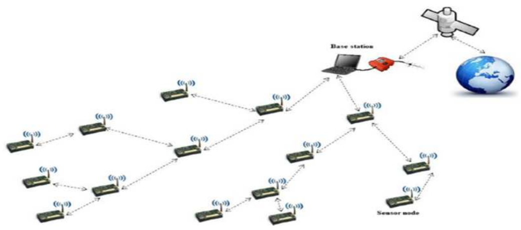

Fig. 1 [17]: A typical wireless sensor network (WSN)

Each sensor node is typically made up of parts like, a microcontroller, a radio transceiver, a battery, etc. The size of a sensor node can be as small as a speck of dust or can be as huge as a shoebox or anywhere in between. The constraints on resources like computational speed, memory, communication bandwidth and energy impose constraints on the size and the cost of deployment of sensor nodes in a Wireless Sensor Network. Fig. 2 shows the basic architecture of a WSN.

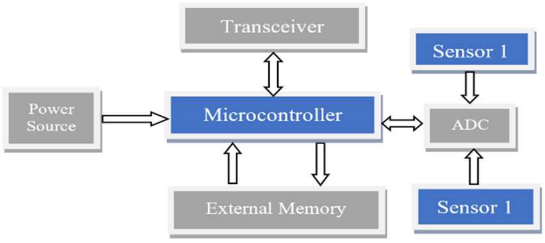

Fig. 2: Architecture of a Wireless Sensor Network

II. Applications of WSNs

There are many possible areas for application of WSNs.

A. Broad categories of WSN applications

Major categories of WSN applications are shown in Fig. 3.

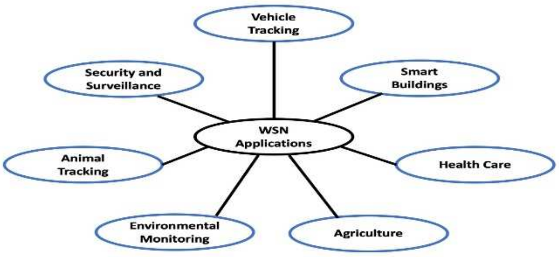

Fig. 3 [5]: Applications of Wireless Sensor Networks

WSNs have diverse objectives in these varied fields [5]. Some of these are as follows:

1. **Health care industry [8]:** To track vitals and other parameters for health monitoring to enable at-home healthcare treatments and telemedicine through wireless body area networks with wearable sensors
2. **Agriculture [9]:** To track physical values such as temperature, soil conditions, humidity, etc to ensure optimal crop conditions in technology driven

precision agriculture to maximise production while minimizing the impact on the environment

3. **Smart buildings and smart homes [10]:** To offer home security and integrated systems with lighting control systems, remote control of connected devices, energy consumption management, remote medical care systems and security

4. **Target tracking ([11] and [12]):** To detect, track and monitor any target (vehicles, animals, etc), which can be used for diverse applications such as coverage sampling of large and inaccessible areas (deep ocean, etc.), road surface monitoring (for pothole detection), tracking of endangered species, etc.

B. WSNs for military applications ([13] and [6])

WSNs also provide security and surveillance, and in the field of the military, the three main categories of applications are as follows [13]:

1. **Battlefield surveillance applications**: These utilize low-cost common motes (another term for nodes) to sense acoustic and magnetic signals produced by different moving targets, which can enable detection and classification of targets (vehicles or troops).

2. **Combat monitoring:** It uses acoustic sensor arrays to detect signals from moving vehicles and gunfire while locating the source. They can also employ a system of Body Sensor Networks (BSNs) for soldiers to perform real-time health monitoring.

3. **Intruder detection:** This can be done with the help of seismic sensors and unattended acoustic sensors which will detect sounds and vibrations of intruders.

These applications make use of a variety of sensors [6] to detect intrusion, chemical or other substances & the distance from objects of interest and for imaging purposes. These include sensors like infrared sensors, RADAR, laser and acoustic, vibration, LIDAR, and various chemical sensors.

III. SECURITY IN WIRELESS SENSOR NETWORKS

In this section, security goals, types of attacks and various countermeasures are discussed.

A. Security Goals in WSNs

Security goals in WSNs [16] include:

Integrity: This ensures data isn't modified (in transmission).

Confidentiality: Information should only be accessible by the intended recipient.

Availability: It offers insurance over reactivity and response time for data transmission (from source to destination).

Freshness: This ensures that data is recent and not outdated, or that no enemy nodes are replaying old messages.

Authentication: Receiver nodes should ensure that the data received is from a legitimate source and not from enemy nodes.

Access Control: Additional verified participants can be given access to read messages.

Non-repudiation: Sensor nodes that transmit a message cannot deny that they sent it, there should be ownership of all transmissions in the WSN.

Self-organisation [15]: In the case of network changes or node destruction, nodes are required to self-repair and organise, which involves the security mechanisms themselves.

Time synchronisation: Applications of WNSs need time synchronisation (of transmission, etc)

B. Attacks in WSNs and countermeasures

Types of attacks in WSNs are as follows:

1. **Internal attacks** [15]: These attacks are caused when enemies hijack nodes by the following mechanisms:

   a. Capturing, reprogramming unattended sensor nodes

   b. Breaching sensor security mechanisms and embedding malicious code to enable hijacking by computationally powerful attackers

   c. Replacing original sensor nodes by fake nodes (obtaining single key or node ID can enable attack of larger set of nodes)

2. **External attacks**: These attacks are by entities outside the network. External attacks are of two main types:

   a. **Passive attacks or eavesdropping**: An attacker listens in on data transmissions to obtain confidential information. This attack is simple to perform since it only requires a receiver to listen in; it does not involve any modifications to this data and therefore cannot be detected easily.

   b. **Active attacks** [16]: An attacker attempts to modify or remove messages transmitted, replay older messages, or even inject false messages into the WSN. Some examples of active attacks are:

      i. **Black hole attack (BLA):** Creation of a sink by falsifying routes to create a "black hole"

      ii. **Wormhole attack:** Attackers at various ends of the network use a tunnel to receive messages and replay them in different parts.

      iii. **Jamming:** Disruption of the channel itself by sending interfering wireless signals thereby reducing the signal-to-noise ratio at the receiver

      iv. **Sybil attack:** The attacker creates many pseudonymous identities and participates in distributed algorithms (elections) to obtain disproportionately large influence

      v. **Tampering:** Attacker obtains physical access to the node to gather cryptographic keys, etc.

      vi. **Selective forwarding:** Malicious nodes in the system "selectively forward" messages and drop certain messages.

      vii. **HELLO flood attack:** An attacker can flood the network with "HELLO" packets used to establish routing protocols to disrupt exchange of other relevant messages.

      viii. **Exhaustion:** Draining energy of a node through calculations or unnecessary data transmission

ix. **Identity replication attack:** Cloning of nodes (creating multiple nodes with the same identity) to collect data

x. **Blackmail attack:** Malicious nodes state that legitimate nodes have been compromised to remove them from the network. Removal of numerous legitimate nodes can disrupt the entire network.

Most common architectures in WSNs [7] follow the OSI model. The relevant layers for WSNs are the physical, data link, network, transport, and application layers. Fig. 4 shows the OSI layers for a WSN.

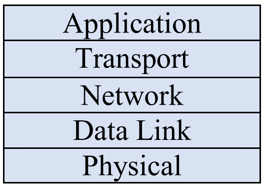

Fig. 4: OSI Model in WSNs

Table I shows the various types of attack in each OSI layer as well as possible security measures.

TABLE I. ATTACKS ON WSNs AND COUNTERMEASURES

Layer	Attack	Security Measure
Physical layer	Jamming	Spread spectrum communication Assigning priority to messages Lowering of duty cycle Region mapping
	Physical attack	Tamper proof hardware; hiding
Data Link Layer	Collision	Use of Error-correcting code Limiting rate of transmission Transmission of smaller packets
	Unfairness	
	Exhaustion attack	Transmission of smaller packets, correction techniques for requesting packet retransmission
Network	Black Hole	Authentication of all messages and identity of source nodes Monitoring transmission with watchdog nodes Probing by periodically sending packets to detect broken links/routes, compromised nodes Redundancy by sending same packets on different routes Egress filtering Verification of bidirectional link
	Selective Forwarding	
	Sybil attack	
	HELLO flood	
	Wormhole	
	Identity replication	
Transport layer	SYN Flooding	Client puzzles and authentication
	Desync attack	Use of SYN cookies

Source: Y. Wang, G. Attebury, and B. Ramamurthy, IEEE Communications Surveys and Tutorials

IV. RELATED WORKS

Yuxin Liu et al. [1] proposes a scheme called ActiveTrust that aims at countering the phenomenon in WSNs called the Black Hole Attack. In a Black Hole Attack, the adversary attacks a node and compromises it. This results in all the packets being routed via this node to be dropped. Sensitive data that was intended for the sink might be lost. Owing to the fact that the network makes decisions based on the data sensed by the nodes, the loss of data due to Black Hole Attack might cause the network to either make the wrong decisions or to completely fail. In this paper, a scheme called ActiveTrust is being proposed to detect and augment trust routing and thereby increase security. The security and efficiency of data routing can be enhanced by speedy detection and gaining nodal trust. In this scheme, multiple detection routes are used. A network of radius 500m with 1000 nodes among which some are black nodes (bad nodes) was used. The results state that when number of deployed black nodes was 300, 400 and 500, it took 5, 9 and 12 rounds respectively, to detect them, which in turn shows that ActiveTrust can detect black nodes quickly, within just a few rounds of detection. Only the residual energy of the nodes is used to establish routes, which leads to a considerable reduction in energy spent as well as the longevity of the network itself. In a network of radius 400m with 400 black nodes among a total of 1000 nodes, the following statistics were seen (respectively) – as the distance from the sink increased from 0 to 300m, for 1 round of detection, the energy consumption ranged approximately between 0 and 4000 nJ with a peak of 4500 nJ at 100m from the sink, for 2 rounds of detection, the energy consumption ranged approximately between 200 and 9000nJ with a peak of 9000 nJ at 100m from the sink and for 3 rounds of detection, the energy consumption ranged approximately between 900 and 13000nJ with a peak of 15000 nJ at 100m from the sink. The following graph in Fig. 5 depicts the above description.

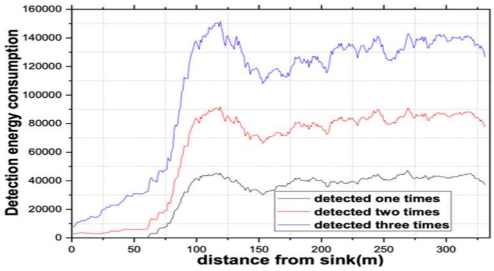

Fig. 5 [1]: Detection energy consumption at distances from the sink

It was also observed that the security performance and the success routing probability increased with this scheme when compared to methods researched earlier. Fig. 6 shows the energy consumption comparison under different schemes.

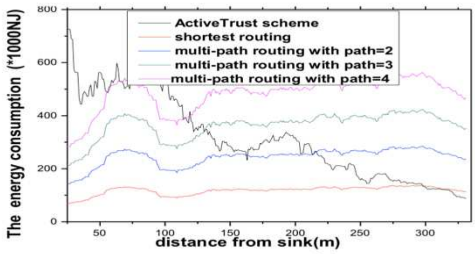

Fig. 6 [1]: Comparison of energy consumed by different schemes

Fig. 7 shows the probability of successful routing for different BLAs.

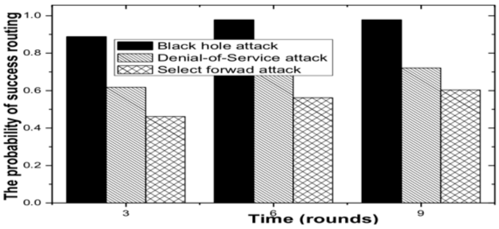

Fig. 7 [1]: Probability of successful routing for different BLAs

The most noteworthy difference between ActiveTrust and older methods is claimed to be the active detection routes created using residual energy. The outcome of having active detection is that if an intruder tries to tap/tamper with the link, they will be exposed. While this allows such an energy-intensive approach to be used in WSNs, if the number and location of nodes with residual energy are not favourable to establish active detection routes, the ActiveTrust mechanism cannot be used at all. And the nodes having residual energy need not be the same over time. Changes in routes or number of nodes or requirement might result in a node which previously had residual energy to be considered a part of a hotspot in the WSN. In such a case, detection routes have to be established every time any change is made to the WSN. Furthermore, ActiveTrust works by establishing multiple active detection routes. Since active detection cannot be applied to every single link in a WSN, the security that this method provides is heavily dependent on the number of active detection routes that can be established without draining the nodes' energy. The other main outcome is transmitting information via nodes that have high nodal trust. If one or more trusted nodes are targeted by an attacker using Identity Replication Attack, the information that gets transmitted would directly end up with duplicate nodes that don't belong to the WSN, which might eventually lead to a BLA. Additionally, this paper emphasises the fact that security will be increased if information is transmitted to a trusted node via a detection route. If information being sent is inside a WSN hotspot where there is no energy to spare, the transmission of data cannot necessarily be via detection routes because either there are no detection routes owing to absence of residual energy or there are very few detection routes in which case these routes will get bombarded with data and hence will reduce lifetime of all nodes and links associated with the transmission. And to add to it, if the distance between the source node and the sink is high, it cannot always be guaranteed that the information being sent will always be routed via detection routes end to end. If, as mentioned earlier, a series of trusted nodes become prey to Identity Replication Attack, all data routed to these duplicate nodes are completely in the control of the attacker. If the attacker drops some of the information and sends the rest forward, the WSN would be under Selective Forwarding attack and so on. ActiveTrust can fare well against direct BLAs in most cases but will not hold up under indirect BLAs.

Yulong Zou et al. [3] discusses a type of attack referred to as an eavesdropping attack and also analyses the response and behavior of WSNs to such an attack. Although primarily aimed at protecting Industrial sensor networks, this scheme counters eavesdropping attack, which is more often than not, one of the most common attacks on any Wireless Sensor Network. In a military scenario, a successful eavesdropping attack can endanger the entire network. An eavesdropping attack refers to a situation in which an unauthorized user listens in on the talk between sensors in a wireless sensor network. This attack can occur in wired or wireless sensor networks. It is more effective and easier to attack a wireless sensor network in this manner. Fig. 8 shows an industrial WSN containing a sink and N sensor nodes in the presence of an eavesdropper.

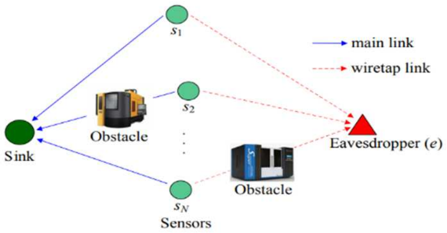

Fig. 8 [3]: Industrial WSN containing a sink and N sensor nodes in the presence of an eavesdropper

While cryptographical techniques can, in most cases, prevent an eavesdropper from listening in, all that is required to crack this encryption is a thorough key search which would require massive computational effort. To patch this loophole, physical layer security mechanisms use the characteristics of the physical medium of the wireless communication to protect the confidentiality of the data going back and forth between sensors present in a WSN. This paper discusses sensor scheduling schemes in industrial applications of WSNs with a single sink node connected to multiple sensor nodes (with an eavesdropper). To characterize the channel in the industrial WSN, the Nakagami model is employed (a type of complex fading model). This method is highly advantageous due to the reduction of energy consumed as well as enabling simpler implementation of the overall system. It requires multiple sensors to be available to choose from to send the data using the proposed optimal scheduling scheme. All nodes are treated as equals in terms of condition and assigned function. The method does not mention priority of data packets associated with critical nodes which may be chosen to transmit the required data. The paper considers single antenna model for all calculations. While this gives a good insight into the application of the method, it does not factor in the energy requirements and design complexity when more than one antenna is added. Additionally, some nodes might be over utilized owing to them being chosen as the most secretive nodes to transmit multiple packets of information.

Yansha Deng et al. [2] evaluate WSNs with three tiers through the use of stochastic geometry modelling to identify how physical layer security (referred to as PLS) can be advantageous. Conventional and current cryptographical methods cannot be implemented in a straightforward manner in multi-hop or multi-tier WSNs. Fig. 9 shows a representation of a three-tier (multi-hop) WSN with an eavesdropper.

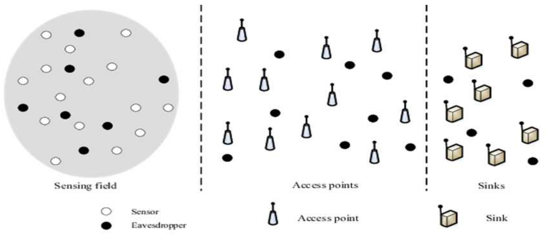

Fig. 9 [2]: Three-tier WSN

A viable lower complexity option for security of data transmitted is physical layer security. In this scheme, physical characteristics of the medium of communication like noise and fading are used to strategically distort the data at the physical layer in order to decrease the odds of an eavesdropper being able to detect that valid data is being transmitted (more often than not, distorted data appears to be irrelevant background noise). In this paper, the concept of stochastic geometry is introduced, which has been utilised to model and monitor where exactly these sensors are located, which is especially important due to the random scattering of these sensors. The development of a novel framework of analysis is performed to inspect how physical layer security can be employed in multi-hop architectures. Compact expressions to determine and quantify secrecy in both connections: sensor to access point and sink to access point were derived on the basis of novel statistical properties. It was thereby proved that implementation of MRC/MRT methods at access points leads to greater security of the data transmitted. Table II summarises the results of the analysis of effect of certain parameters (antennae, access points, sensors and sinks) on secrecy.

TABLE II. EFFECT OF PARAMETERS ON SECRECY

Parameter	**Effect on overall secrecy rate**	**Effect on secrecy rate**	**Reason for relationship**
Multiple antennae at access points	Increases	Increases	Higher diversity
Increasing no. of access points	Increases till critical level, then decreases	Decreases	More access points / targets to attack
Increasing no. of sensors	Decreases	Decreases	Increased interference
Increasing no. of sinks	Increases	Increases	Shorter distance

Multiple antennae at access points are listed as the primary advantage in the analysis done but this will translate to higher complexity in design and deployment along with increased energy consumption. The paper also lists increased number of sinks as an advantage, but this will require additional cost of setup, deployment, and maintenance of sinks.

The paper by Amar Rasheed et al. [4] discusses the development of a framework that can utilise pairwise key pre-distribution and authentication to secure the connection between mobile stations and sensors. In a scenario where the base station is too far from the sensing field, transmission of data over multiple hops can weaken the strength of the security of the data being transmitted. In addition to that, the data can be modified in between, selective forwarding and attacks like, wormhole attack, Sybil attack, sinkhole may be launched. This ultimately leads to corruption and/or loss of data. Traditional schemes used asymmetric keys to counter these problems and provide authenticated data transmission, but the storage and computation cost were too high. In the case of a mobile sink replication attack, pairwise key establishment and authentication is still a problem. If basic schemes are used, deployment of a replicated mobile sink can enable the capture of a substantial fraction of nodes and thereby many keys, thereby gaining control of the entire network. The proposed technique substantially improves the resilience of the network against mobile sink replication attack.

The paper by Jinho Choi et al [14] describes a scheme called distributed detection as a form of physical layer security to secure data transmitted in the WSN. Instead of referring to the secrecy rate, the paper refers to the maximum equivocation in distributed detection in order to evaluate secrecy in the case of an eavesdropping attack. They assumed a system of a WSN with Ally Fusion Centers (AFCs) and an Enemy Fusion Center (EFC). The objective was to ensure reliable data transmission to AFCs without leaking information to the EFC. In a WSN, sensors send local decisions on target state to AFCs, and here at the AFCs are where the final decisions are made. Secured distributed detection can be implemented via two different methods: common randomness (can achieve perfect secrecy and is therefore exploited) and parameter optimization (can't achieve perfect secrecy). Using physical layer techniques that use such properties such as common randomness (of fading) was successfully proved to efficiently secure the data of the WSN through proofs and theorems. There still exist security risks from the physical layer to the transport layer and these possible attacks were not evaluated in this paper. The impact of this security for applications other than distributed detection is also an open point. In addition, the paper only considers two possible channel models (among many other existing channel models) for distributed detection (multiple access channel (MAC) and parallel access channel (PAC)).

The paper by Xiaomei [15] emphasizes the crucial limitations to be considered while selecting the right security protocols for a WSN. These main limitations are limited energy (for nodes to perform data acquisition, processing as well as transmission, which is the most energy intensive), limited capacity (node storage too small to carry out heavy security algorithms), unreliable communication (vulnerable channels), higher communication latency (predominantly in multi-hop architectures due to processing delays), and the fact that nodes are unattended in remote locations (easier to attack). The main sources of WSN attacks are displayed in Fig 10.

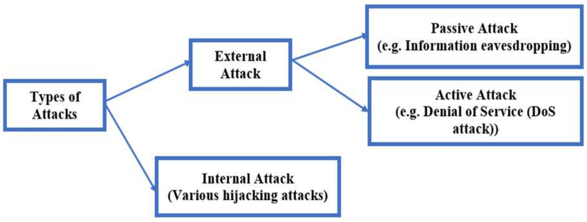
Types of Attacks
External Attack
Passive Attack (e.g. Information eavesdropping)
Active Attack (e.g. Denial of Service (DoS attack))
Internal Attack (Various hijacking attacks)

Fig. 10: Main sources of WSN attacks

It is observed that it is harder to protect WSNs from internal attacks than external attacks. Internal attacks or hijacking of nodes can lead to stolen data, falsified sensor information, route destruction or other disruptive behaviour. Schemes such as RSA (Rivest-Shamir-Adleman encryption) and ECC (Elliptic Curve Cryptography) were deemed too computationally intensive for WSNs and were therefore not applicated to WSNs, however in recent years, some researchers have found that these algorithms can be optimised to reduce energy consumption in order to make them compatible with WSN applications. In addition, there is research ongoing in symmetric cryptographic methods for WSNs since they have many advantages in energy efficiency and computational speed. Xiaomei also discussed possible key management protocols in WSNs. The energy efficiencies of these methods however were not quantified or compared with others.

V. PROPOSED MEASURES

Implementation of only one of the proposed measures mentioned in the referenced papers will not give complete security to WSNs. Multiple layers of security are required for all-round protection. Black hole attack [2] is a 99% sure-fire way of bringing the entire network down. Therefore, to increase data security in the presence of a BLA, active detection-based security and ActiveTrust can be implemented. Previously mentioned methods such as packet splitting and individual routing perform well, but if many routed to the same node then it becomes energy inefficient and therefore impractical. Physical layer security is advantageous-numerical results prove its effectiveness in improving secrecy rate. Interference signals, fading can be exploited to ensure eavesdroppers' reception of signals is stopped (direct fading and interference towards the eavesdropper alone). In three tier WSNs, to avoid mobile sink replication, 2 polynomial pool can be implemented. In 3 tier systems to avoid stationary access node replication, one-way hash chains can be implemented.

VI. CONCLUSION

Data transmitted by WSNs should be secured against numerous types of attacks possible for the system to operate reliably. Therefore, a unique combination of the security measures mentioned must be incorporated to design the most robust, effective system. The designed systems can be judged as per the unique requirement of the application based on a selected set of parameters such as energy efficiency, rate of secrecy, robustness of the system and resistance level to various types of attacks. Physical layer security has been identified as an energy efficient option for securing communication over WSNs.

REFERENCES

[1] Y. Liu, M. Dong, K. Ota and A. Liu, "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 2013-2027, Sept. 2016, doi: 10.1109/TIFS.2016.2570740.

[2] Y. Deng, L. Wang, M. Elkashlan, A. Nallanathan and R. K. Mallik, "Physical Layer Security in Three-Tier Wireless Sensor Networks: A Stochastic Geometry Approach," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1128-1138, June 2016, doi: 10.1109/TIFS.2016.2516917.

[3] Y. Zou and G. Wang, "Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack," in IEEE Transactions on Industrial Informatics, vol. 12, no. 2, pp. 780-787, April 2016, doi: 10.1109/TII.2015.2399691.

[4] A. Rasheed and R. N. Mahapatra, "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks," in IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 5, pp. 958-965, May 2012, doi: 10.1109/TPDS.2010.185.

[5] S. R. Jino Ramson and D. J. Moni, "Applications of wireless sensor networks — A survey," 2017 International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology (ICEEIMT), 2017, pp. 325-329, doi: 10.1109/ICIEEIMT.2017.8116858.

[6] M. P. Đurišić, Z. Tafa, G. Dimić and V. Milutinović, "A survey of military applications of wireless sensor networks," *2012 Mediterranean Conference on Embedded Computing (MECO)*, 2012, pp. 196-199.

[7] Alkhatib, Ahmad A. A. and Gurvinder S. Baicher. "Wireless Sensor Network Architecture.", 2012 International Conference on Computer Networks and Communication Systems (CNCS 2012) IPCSIT vol.35, pp 11-15.

[8] Sadiku, Matthew & Eze, Kelechi & Musa, Sarhan. (2018). Wireless Sensor Networks for Healthcare, Journal of Scientific and Engineering Research, 2018, 5(7):210-213

[9] M. R. Mohd Kassim, I. Mat and A. N. Harun, "Wireless Sensor Network in precision agriculture application," 2014 International Conference on Computer, Information and Telecommunication Systems (CITS), 2014, pp. 1-5, doi: 10.1109/CITS.2014.6878963.

[10] Çetinkaya, Oktay & Akan, Ozgur. (2016). Use of Wireless Sensor Networks in Smart Homes, Emerging Communication Technologies Based on Wireless Sensor Networks, 2016, pp. 233-258, 10.1201/b20085-13.

[11] Bin Zeng and Lu Yao, "Study of vehicle monitoring application with wireless sensor networks," 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015), 2015, pp. 1-4, doi: 10.1049/cp.2015.0747.

[12] G. Padmavathi, D. Shanmugapriya and M. Kalaivani, "A Study on Vehicle Detection and Tracking Using Wireless Sensor Networks," Wireless Sensor Network, Vol. 2 No. 2, 2010, pp. 173-185. doi: 10.4236/wsn.2010.22023.

[13] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: An up-to-date survey," Applied System Innovation, vol. 3, no. 1, p. 14, 2020.

[14] J. Choi, J. Ha and H. Jeon, "Physical layer security for wireless sensor networks," 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2013, pp. 1-6, doi: 10.1109/PIMRC.2013.6666094.

[15] Yang Xiaomei and Ma Ke, "Evolution of wireless sensor network security," 2016 World Automation Congress (WAC), 2016, pp. 1-5, doi: 10.1109/WAC.2016.7583032.

[16] M.-L. Messai, "Classification of Attacks in Wireless Sensor Networks," International Congress on Telecommunication and Application, 2014.

[17] D. E. Boubiche, S. Athmani, S. Boubiche, and H. Toral-Cruz, "Cybersecurity issues in wireless Sensor Networks: Current challenges and solutions," Wireless Personal Communications, vol. 117, no. 1, pp. 177–213, 2020.