International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195370

Identification of Security Threats and Proposed Security Mechanisms for Wireless Sensor Networks

Anusha Medavaka
Software Programmer, Seven Hills IT Solutions LLC, New Jersey

ABSTRACT

The serious constraints and requiring deployment atmospheres of wireless sensor networks make safety for these systems extra difficult than for traditional networks Nevertheless, a number of residential or commercial properties of sensor networks may help address the challenge of building safe and secure networks. The distinct aspects of sensor networks may enable novel defenses not available in traditional networks.In this paper, we examine the security related concerns and also obstacles in wireless sensor networks. We identify the safety and security threats, testimonial suggested protection devices for wireless sensor networks.

Keywords : Security, Wireless Sensor Networks (WSNs), Threats

I. INTRODUCTION

Wireless sensor network (WSN) is a heterogeneous system combining thousands to countless tiny, affordable sensor nodes with numerous differentiating attributes It has extremely low handling power and radio varieties, allowing really low energy consumption in the sensor nodes, and executing restricted as well as particular picking up and also keeping track of functions [2], [3], [4], [5], [6], [7] However, WSNs form a certain class of ad hoc networks that run with little or no framework as well as have attracted scientists for its growth and lots of possible noncombatant as well as armed forces applications such as environmental tracking, battlefield security, and homeland safety and security. In numerous vital military as well as commercial applications, it is critical to secure a sensor network from destructive attacks, which provides a demand for giving protection systems in the network [1] Nevertheless, making safety procedures is a tough task for a WSN due to the following one-of-a-kind qualities.

- Wireless networks are open to every person and has a radio interface configured at the very same regularity band. Therefore, anyone can keep an eye on or join the communication in a wireless channel. This supplies a hassle-free means for attackers to break into a network.

- As in the case of the Internet, most procedures for WSNs do not consider essential safety mechanisms at their design phase. On the various other hand, many protocols are publicly known as a result of the needs for standardization. For these reasons, attackers can conveniently launch attacks by exploiting protection holes in those protocols.

- The constrained sources in sensor nodes make it extremely difficult to implement solid protection algorithms on a sensor system due to their intricacy. Additionally, large numbers of sensor nodes present the need for simple, versatile, as well as scalable security protocols.

- A stronger safety method sets you back a lot more resources in sensor nodes, which can bring about the performance destruction of applications. In most cases, a trade-off needs to be made between safety and security and also efficiency. Nonetheless, weak safety and security protocols may be easily broken by attackers.

A WSN is generally deployed in aggressive areas without any fixed facilities. It is hard to carry out continuous security after network deployment. As a result, it may encounter numerous potential attacks.

II. SECURITY ISSUES IN WSN

A sensor network is a special kind of Ad hoc network. So it shares some usual home as local area network. There are generally a number of protection needs to secure a network [1] These demands ought to be taken into consideration throughout style of a safety and security protocol, including confidentiality, integrity, and also authenticity. An efficient safety and security method ought to give solutions to meet these requirements. The protection needs [1], [8], [9], [10], [11], [12] of a wireless sensor network can be identified as follows:

A. Data Confidentiality

Data confidentiality in networking is most challenging job in network security. The significant trouble is that radio range is an open resource and can be made use of by any person furnished with proper radio transceivers. An assaulter can eavesdrop on the packets transferred in the air as long as he has the ability to keep an eye on the radio channels utilized in the communication. An assaulter can capture a node, go into it with special devices, and also locate helpful data. The enemy can likewise derive the keys in a node without recording it, which can be done by assessing the secret data gathered from various other jeopardized nodes and/or package method data systems (PDUs). Under the enemy's control, the brand-new endangered node can be used to introduce even more malicious attacks.Confidentiality is a guarantee of certified accessibility to information. It is the capability of the network to hide messages from an easy enemy to ensure that any kind of message connected using the sensor network continues to be confidential [13] Hence, it makes certain the defense of delicate details and not disclosed to unauthorized third parties. Applications like monitoring of details, industrial keys and also crucial distribution need to depend on confidentiality. In such applications, nodes communicate highly sensitive data. The typical strategy for maintaining confidentiality is to encrypt the data with a secret trick that just desired receivers have, therefore achieving confidentiality. As per TinySec [17], cipher block chaining (CBC) is the most appropriate security system for sensor networks.

B. Data Authenticity

In addition to modifying existing packets, an aggressor can directly inject packets if he recognizes the packet layout specified in the network method pile. The infused packets can carry false info, which might be approved by getting nodes. Applications deployed in a WSN, for instance, environmental monitoring or item tracking, can be interfered with by the incorrect details. Transmitting protocols can fail as a result of the incorrect routing information. The Sybil attack [15] is a case in point of package injection.Data authenticity is a guarantee of the identities of connecting nodes. WSN connects sensitive data to assist in many important choices making. Thus, it is extremely essential for each node to know that an obtained packet originates from an actual sender. Otherwise, the obtaining node can be cheated into doing some incorrect actions. Likewise, authentication is necessary during exchange of control information in the network. The basic approach for keeping authenticity is with using message authentication code, obstacle response, trademark, verifying public key, program and also multicast authentication, and so on

C. Data Integrity

Transmission mistakes are integral in wireless communications because of the instability of wireless networks, which results from several reasons, for instance, network fading, time- regularity comprehensibility, and also inter-band interference. Mistakes can also happen in each forwarding node since no electronic devices are perfect. When the operation conditions, as an example, temperature level or humility, are out of the normal range, electronic devices can run into malfunction, which can cause mistakes in packets. Those mistakes might not be observed by the forwarding node and also thus those mistake packages may still be sent out, creating troubles at down- stream nodes. In aggressive environment, data en route can additionally be transformed by an assailant who can change a packet before it gets to the receiver. This can create lots of problems. The aggressor can simply introduce radio disturbance to some little bits in transmitted packets to change their polarities. The unintelligible packets will certainly be dropped at the receiver, leading to an easy Denial of Service (DoS) strike [14] A lot more severe damages can be caused if the enemy comprehends the package layout as well as the semantic definition of the communication procedure. In that situation, the enemy can modify a package to change its content to make sure that the receiver acquires incorrect info. In a WSN, for instance, a package containing the area of a crucial occasion can be changed to ensure that a wrong area is reported to the base terminal. Control as well as management packages can be changed to ensure that nodes have inconsistent understanding on the network geography, which triggers numerous directing troubles. A package bearing errors is worthless as well as creates added processing at the sender and also the receiver. Data integrity is to make certain that info is not changed in transit, either due to destructive intent or by accident. Thus, integrity is a guarantee that packages are not modified in transmission. This is a fundamental requirement for interactions because the receiver needs to know precisely what the sender desires her to recognize. Nevertheless, this is not a very easy task in wireless communications. The basic method for making certain data integrity is via the use of message integrity code, etc.

Data Freshness

All info defines a short-lived standing of a things and also hence stands in only a limited time interval. For that reason, when a node receives a packet, it needs to be ensured that the packet is fresh. Otherwise, the package is pointless because the information shared in it is invalid. Packet replaying is a major danger to the freshness requirement in network communications. An attacker can intercept a package from a network, hold it for any type of amount of time, and after that reply it into the network. The out-dated details had in the package can create many issues to the applications deployed in the network. In a WSN, as an example, a package suggesting the emergence of an occasion will conflict with an old packet consisting of no indication of the event. If some old directing control packages are replayed, sensor nodes will be put into a disorder regarding the network topology and therefore the transmitting protocol will stop working. Along with the replay in time measurement, packets can also be repeated precede dimension. An instance is the Wormhole strike in WSNs [16] Hence, even if confidentiality and data integrity are assured we additionally need to make certain the freshness of each message. Data freshness suggests that the data is current, and it guarantees that no old messages have actually been repeated. In order to ensure the freshness of package, a timestamp can be attached to the package. A getting node can compare the timestamp in the package with its own time clock as well as establish whether the packet stands or not

D. Availability

Sensor nodes might lack battery power as a result of excess computation or interaction and become inaccessible. It might occur that an assaulter might jam interaction to make sensor(s) inaccessible. The demand of safety and security not just influences the operation of the network, yet additionally is extremely crucial in maintaining the availability of the network. Any kind of trouble in a network can lead to the degradation of the network functionality as well as thus jeopardize the network availability, leading to the DoS [14] Availability is an assurance of the ability to give expected solutions as they are developed in advance. It is an extremely detailed principle in the feeling that it belongs to virtually every facet of a network. The basic strategy for keeping confidentiality is with the use of discerning forwarding, multipath directing, etc

..

III. SECURITY THREATS AND ATTACKS IN WSN

A.Security Threats

A hazard is a situation or event with the possible to adversely affect a system through a safety violation as well as the chance that an attacker will certainly manipulate a specific vulnerability, causing damage to a system property is called danger. There can be lots of prospective threats to WSNs, as an example, power drain, physical meddling, termination when implementation as a result of the hostile setting or deliberate efforts to overturn a node by breaching the safety and security. The classifications of the threats might be (a) Passive Information Gathering, (b) Subversion of node or Insertion of an incorrect node, (c) node malfunction, (d) node interruption, (e) message corruption, (f) denial of solution, or(g) website traffic evaluation [22]

According to Karlof et. al. [19], threats in wireless sensor network can be categorized into the following groups:

External versus internal attacks: The exterior (outsider) attacks are from nodes which do not come from a WSN. An exterior opponent has no accessibility to most cryptographic products in sensor network. The interior (expert) attacks take place when genuine nodes of a WSN act in unexpected or unapproved means. The inside attacker might have partial crucial product and the depend on of other sensor nodes. Inside attacks are much tougher to find. Outside attacks might trigger passive eavesdropping on data transmissions, in addition to can reach infusing fraudulent data right into the network to take in network sources as well as elevate Denial of Solution (DoS) assault. Whereas within assaulter or internal danger is a certified participant in the sensor network which has actually gone aggressive. Insider attacks may be mounted by either compromised sensor nodes running destructive code or adversaries that have actually taken the essential product, code, as well as data from genuine nodes as well as who then utilize several laptop-class devices to assault the network.

- Easy versus energetic attacks: Passive attacks remain in the nature of eavesdropping on, or surveillance of packages traded within a WSN. The active attacks entail some modifications of the data vapor or the creation of a false stream in a WSN.

- Mote-class versus laptop-class attacks: In mote-class (sensor-class) attacks, an opponent attacks a WSN by utilizing a few nodes with similar capabilities as that of network nodes. In laptop-class attacks, an enemy can make use of extra effective devices like laptop, and so on and can do far more harm to a network than a harmful sensor node. These sorts of attackers can jam the radio link in its immediate vicinity. An enemy with laptop-class devices have greater battery power, a more capable CPU, a high- power radio transmitter, or a sensitive antenna and thus they can affect much more than an opponent with only normal sensor nodes. A single laptop-class aggressor could be able to be all ears on an entire network.

B. Attacks

Wireless networks are a lot more susceptible to protection attacks than wired networks, because of the program nature of the transmission tool. These attacks are generally as a result of several vulnerabilities at the various layers in the network [22] Furthermore, wireless sensor networks have an extra vulnerability because nodes are commonly positioned in an aggressive or dangerous atmosphere where they are not physically safeguarded [21] The security of the WSNs is jeopardized as a result of the attacks. An attack can be defined as an attempt to acquire unapproved accessibility to a solution, a source or information, or the attempt to endanger integrity, availability, or confidentiality of a system [12] Attackers, intruders or the opponents are the begetter of an attack. The weak point in a system safety style, execution, setup or restrictions that could be made use of by attackers is known as vulnerability or defect. As shown in Number 1, attacks on the computer system or network can be broadly identified [18] as interruption, interception, modification and also manufacture

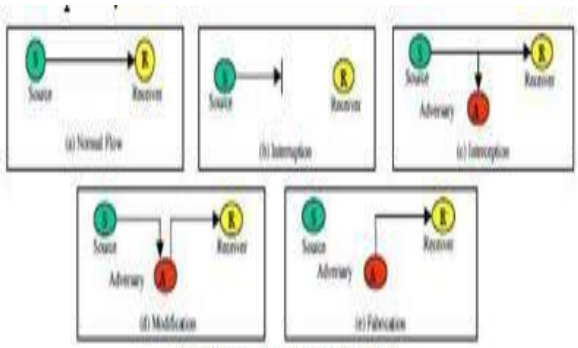


Fig. 1 Attack security classes

Interruption is an attack on the availability of the network, as an example physical capturing of the nodes, message corruption, insertion of malicious code etc. Interception is an attack on confidentiality. The sensor network can be jeopardized by an opponent to acquire unauthorized access to sensor node or data stored within it. Modification is a strike on integrity. Adjustment means an unauthorized celebration not just accesses the data but tampers it, for example by modifying the data packets being transferred or creating a rejection of service strike such as swamping the connect with phony data. Construction is an assault on authentication. In fabrication, an opponent infuses incorrect data and also compromises the credibility of the details communicated. Several of the essential attacks [12], [26], are categorized as follows:

Rejection of Service (DoS).

Rejection of Service (DoS) [23], [27], [28] is created by the unintentional failure of nodes or destructive action. This attack is a prevalent hazard to a lot of networks. Sensor networks being really energy-sensitive and also resource-limitation, they are very vulnerable to DoS attacks. Wood and also Stankovic [14] discovered various DoS attacks that might occur in every network layers of sensor networks. The most basic DoS strike tries to wear down the sources readily available to the target node, by sending added unneeded packages as well as hence stops genuine network individuals from accessing services or sources to which they are entitled. DoS attack is meant not just for the adversary's effort to subvert, interrupt, or ruin a network, yet alsoforanyeventthatdiminishesa network's ability to supply a service. In wireless sensor networks, several kinds of DoS attacks in different layers may be performed.AtphysicallayertheDoS attacks could be obstructing as well as meddling, at link layer, collision, exhaustion, unfairness, at network layer, disregard and also greed, homing, misdirection, black holes as well as at transport layer this assault can be executed by malicious flooding and de-synchronization. Sybil.

Sybil assault is specified as a harmful device illegitimately handling multiple identifications. In Sybil strike [24], an opponent can appear to be in multiple locations at the exact same time. Simply put, a single node presents several identifications to other nodes in the sensor network either by making or taking the identities of legit nodes. Figure 2 demonstrates Sybil assault where a foe node 'AD' is present with multiple identities. 'AD' appears as node 'F' for 'A', 'C' for 'B' and also 'A' regarding 'D' so when 'A' wants to connect with 'F' it sends the message to 'ADVERTISEMENT'. Sybil attack is a damaging risk to sensor networks. It poses a significant risk to geographical directing methods, where place conscious routing requires nodes to trade coordinate details with their neighbors to effectively course geographically resolved packets. The Sybil strike can interfere with typical functioning of the sensor network, such as multipath transmitting, utilized to check out the numerous disjoint courses in between resource-.

location pairs. It can substantially reduce the efficiency of mistake tolerant systems such as distributed storage space, dispersity and

multipath.

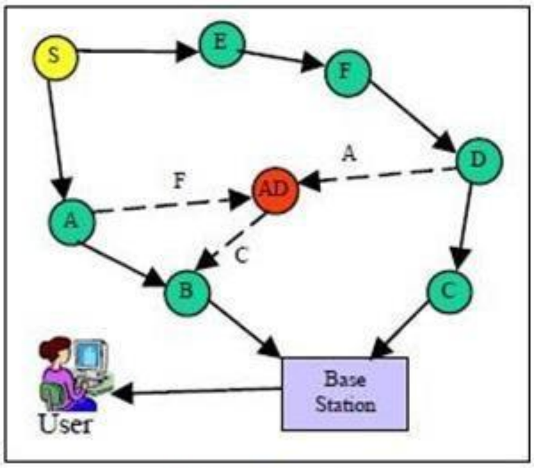


Fig. 2 Sybil attack

Sybil strike problem was initial offered in the peer-to-peer dispersed systems by Douceur [24] wherein it was explained that it can defeat the redundancy devices of the dispersed storage systems. Newsome et al. [15] assessed the risk presented by the Sybil attack to wireless sensor networks. They developed a classification of different kinds of the Sybil assault, recommended a number of methods to defend against the Sybil strike, and also examined their efficiency quantitatively.Sybil attack tries to break down the integrity of data, safety and security as well as source utilization that the distributed algorithm efforts to achieve. It can be executed for attacking the dispersed storage space, transmitting system, data aggregation, ballot, reasonable source appropriation as well as wrongdoing discovery [15] Primarily, any peer-to-peer network (specifically wireless ad hoc networks) is susceptible to sybil strike.

Sinkhole (Blackhole): In sinkhole attacks, a malicious node acts as a blackhole [29] to draw in all the traffic in the sensor network with a jeopardized node producing a symbolic sinkhole with the adversary at the center. A jeopardized node is put at the centre, which looks eye-catching to surrounding nodes and also lures nearly all the website traffic predestined for a base station from the sensor nodes. Hence, developing a symbolic sinkhole with the foe at the center, from where it can attract the most traffic, perhaps closer to the base station to ensure that the destructive node can be perceived as a base station. Figure 3 demonstrates sinkhole attack where 'SH' is a sinkhole. This sinkhole draws in web traffic from almost all the nodes to thrashing via it.

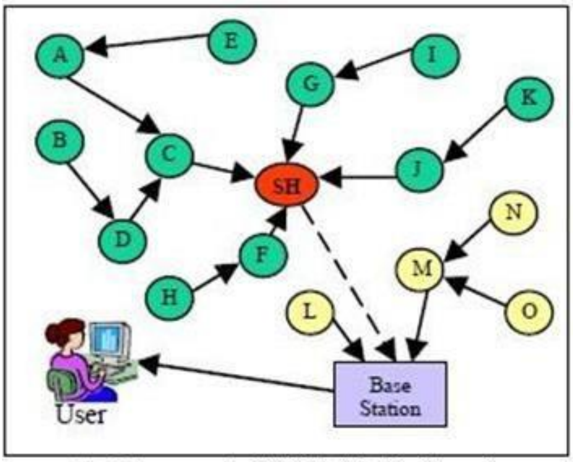


Fig. 3 An example of Sinkhole (Blackhole) attack

The main reason for the sensor networks susceptible to sinkhole attacks is due to their specialized communication pattern. Sinkholes are challenging to protect in protocols that use advertised information such as continuing to be energy or a price quote of end-to- end dependability to create a transmitting topology since this details is hard to confirm.

Hello flood: Hey there flood strike [19] uses HELLO packets as a tool to persuade the sensors in WSN. In this type of attack an opponent with a high radio transmission range (labelled as a laptop-class assailant) and handling power sends out HELLO packets to a variety of sensor nodes which are dispersed in a huge location within a WSN. The sensing units are hence convinced that the foe is their neighbor. This presumption may be incorrect. Consequently, while sending out the information to the base station, the sufferer nodes try to undergo the assaulter as they understand that it is their neighbor as well as are eventually spoofed by the opponent. A laptop- course assaulter with large transmission power can convince every node in the network that the enemy is its next-door neighbor, so that all the nodes will certainly reply to the HELLO message and squander their energy. Number 4 shows how an adversary node 'AD' program hi packets to convince nodes in the network as neighbor of 'AD'. Though some node like I, H, F are away from 'AD' they believe 'ADVERTISEMENT' as their next-door neighbor as well as attempt to onward packets through it which leads to wastefulness of power and also data loss.

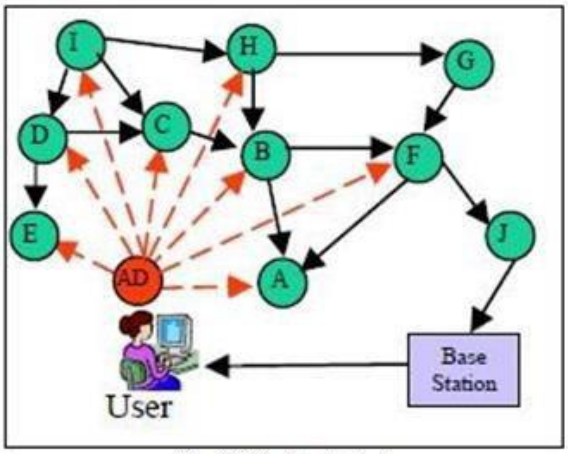


Fig. 4 Hello flood attack

In a HELLO flood attack, every node thinks that the opponent is within one-hop radio interaction range. If the aggressor subsequently advertises affordable paths, nodes will certainly attempt to onward their messages to the assailant. Procedures which depend upon local information exchange in between bordering nodes for geography maintenance or flow control are likewise subject to this attack. HELLO floodings can additionally be considered one-way, broadcast wormholes.

Wormhole: Wormhole attack [16], [25] is a critical attack in which the attacker documents the packets (or little bits) at one area in the network as well as tunnels those to one more place. In the wormhole attack, an adversary (harmful nodes) eavesdrop the packet as well as can passage messages obtained in one part of the network over a low latency link and retransmit them in a different part. This creates a false scenario that the initial sender remains in the community of the remote area. The tunneling treatment forms wormholes in a sensor network. The tunneling or retransmitting of little bits can be done selectively. Figure 5 shows Wormhole attack where 'WH' is the enemy node which develops a tunnel between nodes 'E' and 'I'. These two nodes are present at most range from each other.

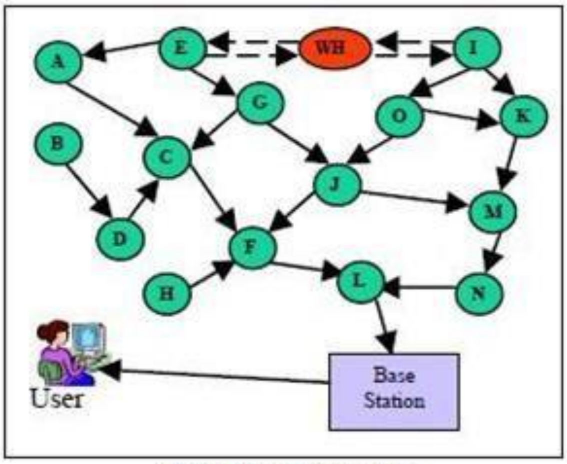


Fig. 5 Wormhole attack

The most basic situation of this attack is to have a malicious node forwarding data in between two legit nodes. Wormholes usually persuade remote nodes that they are next-door neighbors, bring about quick exhaustion of their power sources. Wormholes work even if transmitting info is confirmed or secured. This attack can be introduced by experts and outsiders. This can produce a sinkhole because the enemy beyond of the wormhole can artificially supply a premium quality course to the base terminal, possibly all traffic in the surrounding area will certainly be attracted via her if alternate routes are dramatically much less appealing. When this attack is paired with careful forwarding as well as the Sybil attack it is really tough to detect. Much more generally, wormholes can be made use of to exploit routing race conditions. A transmitting race condition commonly arises when a node takes some action based upon the initial circumstances of a message it obtains as well as ultimately ignores later on circumstances of that message. The goal of this attack is to undermine cryptography protection and also to puzzle the sensor's network protocols.Wormhole attack is a substantial risk to wireless sensor networks, because this kind of attack does not need endangering a sensor in the network instead, it could be performed even at the initial stage when the sensors begin to uncover the neighboring details.

IV. RELATED WORKS AND SECURITY SOLUTIONS IN WSN

In the recent years, wireless sensor network protection has actually been able to draw in the focus of a variety of scientists worldwide [7] Because source constraint on sensor nodes, dimension as well as thickness of the networks, unidentified geography prior to implementation, and also high threat of physical attacks to unattended sensing units, it comes to be really difficult job to use safety and security plans in wireless sensor networks While much research has actually focused on making these networks possible and also helpful, security has gotten little attention. Researchers have actually been attempting to solve safety and security concerns [20] A lot of the existing protection devices need extensive calculation as well as memory. Lots of security devices need duplicated transmission/communication between the sensor nodes which are further reeled in their sources. In this section, we examine a few of the popular safety and security services and also combat a few of the threats to the sensor networks.

1) A.SPINS

Safety and security procedures for sensor networks (SPIN) was proposed by Adrian Perrig et al. [36] in which protection building blocks optimized for source constrained environments and wireless communication. SPINs has two safe foundation: (a) sensor network encryption procedure (SNEP) and (b) μTESLA. SNEP supplies data confidentiality,two-partydata authentication, and data freshness. μTESLA offers confirmed broadcast for severelyresource-constrained environments.SNEP utilizes encryption to achieve confidentiality and also message authentication code (MAC) to attain 2- event authentication and data integrity. Because sending data over the RF network calls for extra energy, all cryptographic primitives such as security, MAC, hash, random number generator, are created out of a solitary block cipher for code reuse. This, together with the symmetric cryptographic primitives utilized minimizes the overhead on the resource constricted sensor network. SNEP provides number of benefits such as low communication expenses, semantic security which prevents eavesdroppers from inferring the message material from the encrypted message, data authentication, replay protection, and message freshness. μTesla is a new protocol which offers authenticated program for severely resource-constrained environments. In a broadcast tool such as sensor network, uneven digital signatures are unwise for the authentication, as they need lengthy trademarks with high interaction overhead. μTesla methods provide efficient validated broadcast [39], [40] and achieves asymmetric cryptography by postponing the disclosure of the symmetric tricks. μTesla constructs verified program from symmetrical primitives, however presents crookedness with postponed key disclosure and one-way function essential chains. μTESLA resolves the adhering to insufficiencies of TESLA in sensor networks:

- TESLA verifies the first packet with an electronic trademark, which is also pricey for our sensor nodes. μTESLA utilizes only symmetrical mechanisms.

- Divulging a key in each package requires excessive energy for sending out as well as obtaining. µTESLA divulges the key as soon as per date.
- It is expensive to save a one-way key chain in a sensor node. µTESLA limits the number of validated senders.

B.TINYSEC

TinySec is link layer protection style for wireless network, which was created by Karlof et al. [17] It provides similar solutions as of SNEP, consisting of authentication, message integrity, confidentiality and also replay defense. It is a lightweight, generic safety plan that can be integrated right into sensor network applications. A significant distinction between TinySec and SNEP is that there are no counters made use of in TinySec. TinySec provides the fundamental safety and security properties of message authentication and also integrity using MAC, message confidentiality via file encryption, semantic safety with an Initialization Vector and also replay defense.

TinySec supports two various safety alternatives: verified security (TinySec- AE) as well as authentication only (TinySec- Auth). For verified file encryption (TinySec-AE), TinySec makes use of cipher block chaining (CBC) mode and secures the data payload and also authenticates the packet with a MAC. The MAC is calculated over the encrypted data as well as the packet header. In authentication just setting (TinySec-Auth), TinySec authenticates the entire package with a MAC, but the data haul is not secured.

C.LEAP

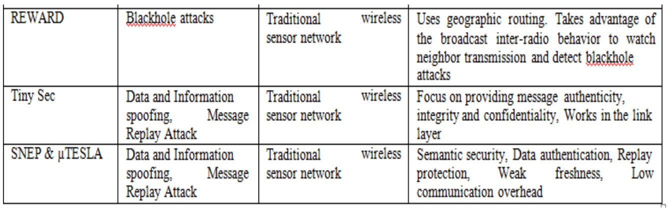
Localized file encryption and authentication protocol (LEAP) Procedure [41] is a vital management protocol for sensor networks. It is developed to sustain in-network processing and also safe and secure communications in sensor networks. LEAP gives the fundamental safety services such as confidentiality and also authentication. Furthermore, LEAP is to fulfill numerous security as well as performance needs that are significantly a lot more difficult to sensor networks. Design of the JUMP method is inspired by the monitoring that various sorts of messages exchanged in between sensor nodes have various security demands. LEAP has the complying with residential or commercial properties:

- LEAP supports the establishment of four

types of keys for each sensor node-- a private essential shared with the base station, a pairwise vital shown to another sensor node, a cluster essential shared with numerous neighboring nodes, and also a team trick that is shared by all the nodes in the network The procedure made use of for developing and also updating these tricks is interaction and power effective, and also decreases the involvement of the base station.

- JUMP consists of an efficient protocol for inter-node neighborhood program authentication based upon the use of one-way vital chains.
- Trick sharing strategy of LEAP sustains source authentication without precluding in- network processing and passive participation. It restricts the safety and security influence of a node compromise to the prompt network neighborhood of the endangered node.

In Table 1, we have actually summarized different security schemes together with their major properties for wireless sensor network.



REWARD	Blackhole attacks	Traditional wireless sensor network	Uses geographic routing. Takes advantage of the broadcast inter-radio behavior to watch neighbor transmission and detect blackhole attacks
Tiny Sec	Data and Information spoofing, Message Replay Attack	Traditional wireless sensor network	Focus on providing message authenticity, integrity and confidentiality, Works in the link layer
SNEP & µTESLA	Data and Information spoofing, Message Replay Attack	Traditional wireless sensor network	Semantic security, Data authentication, Replay protection, Weak freshness, Low communication overhead

V. CONCLUSION

Safety and security is ending up being a significant concern for power constrained wireless sensor network due to the broad security-critical applications of WSNs. Therefore, security in WSNs has actually drawn in a great deal of attention in the recent years. The significant functions of WSNs make it extremely testing to create solid security protocols while still maintaining low expenses. In this paper, we have introduced some security problems, threats, as well as attacks in WSNs and also some of the solutions. Network protection for WSNs is still a very fruitful study direction to be more checked out.

VI. REFERENCES

[1]. Jun Zheng and Abbas Jamalipour, “Wireless Sensor Networks: A Networking Perspective”, a book published by A John & Sons, Inc, and IEEEE, 2009.

[2]. Shio Kumar Singh, M.P. Singh, and D.K. Singh, “A survey of Energy-Efficient Hierarchical Cluster-based Routing in Wireless Sensor Networks”, International Journal of Advanced Networking and Application (IJANA), Sept.–Oct. 2010, vol. 02, issue 02, pp. 570–580.

[3]. Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Energy-efficient Homogeneous Clustering Algorithm for Wireless Sensor Network", International Journal of Wireless & Mobile Networks (IJWMN), Aug. 2010, vol. 2, no. 3, pp. 49-61.

[4]. Shio Kumar Singh, M.P. Singh, and D.K. Singh, “Applications, Classifications, and Selections of Routing Protocols for Wireless Sensor Networks” International Journal of Advanced Engineering Sciences and Technologies (IJAEST), November 2010, vol. 1, issue no. 2, pp. 85-95.

[5]. Shio Kumar Singh, M.P. Singh, and D.K. Singh, “Routing Protocols in Wireless Sensor Networks – A Survey” International Journal of Computer Science and Engineering Survey (IJCSES), November 2011, Vol. 1, issue no. 2, pp. 63-83

[6]. Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Performance Evaluation and Comparison of Energy-efficient Routing Protocols for Wireless Sensor Network", Global Journal of Computer Application and Technology (GJCAT), Jan. 2011, vol. 1, no. 1, pp. 57-65.

[7]. Shio Kumar Singh, M.P. Singh, and D.K. Singh, "Energy Efficient Transmission Error Recovery for Wireless Sensor Network", International Journal of Grid and Distributed Computing (IJGDC), December 2010, vol. 3, no. 4, pp. 89-104.

[8]. Sugandhi Maheshwaram, “A Comprehensive Review on the Implementation of Big Data Solutions” in “International Journal of Information Technology and Management”, Vol. XI, Issue No. XVII, November-2016 ISSN : 2249-4510]

[9]. Sugandhi Maheshwaram , “An Overview of Open Research Issues in Big Data Analytics” in “Journal of Advances in Science and Technology”, Vol. 14, Issue No. 2, September-2017 ISSN : 2230-9659]

[10]. Suresh Kumar Mandala, Neelima Gurrapu, Mahipal Reddy Pulyala, “ A Study on the Development of Machine Learing in Health Analysis”, Indian Journal of Public Health Research & Development, volume 9, Number 12, December 2018, ISSN-0976-0245(Print)-ISSN-0976-5506 (Electronic)]

[11]. Suresh Kumar Mandala,Mahipal Reddy Pulyala and Sanjay Pachouri, “Being a Smart Sapien with Information Centric Networking and Cloud Computing”, International Journal of Pure and Applied Mathematics,Volume 117, No. 21, 2017, 243-255,ISSN: 1311-8080 (printed version)]

[12]. Suresh Kumar Mandala, Sanjay Pachouri, “performance evaluation of multi stage attacks prediction”, Journal of Advanced Research in Dynamical and Control Systems, Vol. 9, September 2017, JARDCS Special Issue On Engineering Technology.

[13]. Thota Mounika, Mandala Suresh kumar, “Document Proximity: Keyword Query

Suggestion Based On User Location”, International Journal of Research, Volume 04, Issue 14, November 2017, e-ISSN: 2348-6848 ,p-ISSN: 2348-795X.

[14]. Syeda Sobia Farees , M. Suresh Kumar, “A Novel Approach for Protecting Location Information in Geosocial Applications “, IJIEMR, Vol 1, Issue 2, November 2016 ISSN:2456-5083]

[15]. Suresh Kumar Mandala,Sanjay Pachouri, “A Reviewed Study on Financial Cyber Crime and Frauds”, International Journal of Advances in Arts, Sciences and Engineering(ijoaase.com), Volume 4 Issue 9, Sep 2016, ISSN. 2320-6144 (Online)]

[16]. Siripuri Kiran, Ajmera Rajesh, “A Study on Mining Top Utility Itemsets In A Single Phase” in “International Journal for Science and Advance Research in Technology (IJSART)”, Volume-4, Issue-2, February-2018, 637-642, ISSN(ONLINE): 2395-1052]

[17]. Yeshwanth Rao Bhandayker, “Security Mechanisms for Providing Security to the Network” in “International Journal of Information Technology and Management”, Vol. 12, Issue No. 1, February-2017, ISSN : 2249-4510]

[18]. Sugandhi Maheshwaram, S. Shoban Babu , “An Overview towards the Techniques of Data Mining” in “RESEARCH REVIEW International Journal of Multidisciplinary”, Volume-04, Issue-02, February-2019 ISSN : 2455-3085]

[19]. Yeshwanth Rao Bhandayker , “A Study on the Research Challenges and Trends of Cloud Computing” in “RESEARCH REVIEW International Journal of Multidisciplinary ”, Volume-04, Issue-02, February-2019 ISSN : 2455-3085]

[20]. Sriramoju Ajay Babu, Dr. S. Shoban Babu, “Improving Quality of Content Based Image Retrieval with Graph Based Ranking” in “International Journal of Research and Applications”, Volume 1, Issue 1, Jan-Mar 2014 ISSN : 2349-0020]

[21]. Dr. Shoban Babu Sriramoju, Ramesh Gadde, “A Ranking Model Framework for Multiple Vertical Search Domains” in “International Journal of Research and Applications” Vol 1, Issue 1,Jan-Mar 2014 ISSN : 2349-0020].

[22]. Mounika Reddy, Avula Deepak, Ekkati Kalyani Dharavath, Kranthi Gande, Shoban Sriramoju, “Risk-Aware Response Answer for Mitigating Painter Routing Attacks” in “International Journal of Information Technology and Management”, Volume VI, Issue I, Feb 2014 ISSN : 2249-4510]

[23]. Sugandhi Maheshwaram, “A Review on Deep Convolutional Neural Network and its Applications” in “International Journal of Advanced Research in Computer and Communication Engineering”, Vol. 8, Issue No. 2, February-2019 ISSN : 2278-1021], DOI 10.17148/IJARCCE.2019.8230

[24]. Yeshwanth Rao Bhandayker. "An Overview : Security Solutions for Cloud Environment." International Journal for Scientific Research and Development 7.2 (2019): 1596-1598.

[25]. Yeshwanth Rao Bhandayker. "AN OVERIEW OF CYBER SECURITY", International Journal of Research, vol. 8, Issue. 3 (2019): 2236-6124.

[26]. Sugandhi Maheshwaram, "A STUDY ON THE CHALLENGES IN HANDLING BIG DATA", International Journal of Research, vol. 8, Issue. 3 (2019): 2236-6124.

[27]. Yeshwanth Rao Bhandayker. "An Overview of Service Models and Cloud Computing Evolution in IT", International Journal of Research and Applications, vol. 5, Issue. 20, Oct - Dec 2018 Transactions 5(20) : 1000-1004. ISSN : 2349 – 0020]

[28]. Yeshwanth Rao Bhandayker. "A Comprehensive Survey on Security Issues and Advantages towards Cloud Computing",

International Journal of Research and Applications, vol. 5, Issue. 18,Apr - Jun 2018 Transactions 5(18): 801-807. ISSN : 2349 – 0020]

[29]. Sugandhi Maheshwaram, . "A Study on Security Information and Event Management (SIEM)", International Journal of Research and Applications, vol. 5, Issue. 17, Jan - Mar 2018 Transactions 5(17): 705-708. ISSN : 2349 – 0020]

[30]. Sugandhi Maheshwaram, . "A Novel Technique for Preventing the SQL Injection Vulnerabilities", International Journal of Research and Applications, vol. 5, Issue. 19, July - Sep 2018 Transactions 5(19): 901-909. ISSN : 2349 – 0020]

[31]. Shoban Babu Sriramoju, "Substantial Overall Performance Pattern-matching Algorithm for etwork Stability", International Journal of Research and Applications, vol. 5, Issue. 17, Jan - Mar 2018 Transactions 5(17): 701-704. ISSN : 2349 – 0020]

[32]. Sugandhi Maheshwaram. "A Study Design of Big Data by Concentrating on the Atmospheric Information Evaluation." International Journal for Scientific Research and Development 7.3 (2019): 233-236.

[33]. Suresh Kumar Mandala,Sanjay Pachouri, “Analytical Study for Intrusion Detection System to Detect Cyber Attack”, Airo International Research Journal, Volume VII, March 2016]ISSN: 2320-3714

[34]. Ranjeeth kumar.M, M.Suresh Kumar, S.S.V.N Sarma, “FUZZY KEYWORD SEARCH IN XML DATA”, International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June 2013 ISSN : 2229-5518]

[35]. Yeshwanth Rao Bhandayker, “AN OVERVIEW OF THEINTEGRATION OF ALL DATA MINING AT CLOUD-COMPUTING” in “Airo International Research Journal”, Volume XVI, June 2018 ISSN : 2320-3714]

[36]. Siripuri Kiran, 'Decision Tree Analysis Tool with the Design Approach of Probability Density Function towards Uncertain Data Classification', International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X,Volume 4 Issue 2, pp.829-831, January-February 2018. URL : http://ijsrst.com/IJSRST1841198

[37]. Yeshwanth Rao Bhandayker , “Artificial Intelligence and Big Data for Computer Cyber Security Systems” in “Journal of Advances in Science and Technology”, Vol. 12, Issue No. 24, November-2016 ISSN : 2230-9659]

Cite this article as :

Anusha Medavaka, "Identification of Security Threats and Proposed Security Mechanisms for Wireless Sensor Networks", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 3, pp. 194-205, May-June 2019.
Available at doi :
https://doi.org/10.32628/CSEIT195370
Journal URL : http://ijsrcseit.com/CSEIT195370