THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

A Review on Security In Wireless Sensor Network

Harwant Singh Arri
hs.arri@lpu.co.in
Computer Science and Engineering
Lovely Professional University
Phagwara, India

Dhiraj Kapila
dhiraj.23509@lpu.co.in
Computer Science and Engineering
Lovely Professional University
Phagwara, India

***Abstract*—** In the modern arena Wireless Sensor Network (WSN) discovers its presence in every domain area precisely the the areas of medicine & health care, armed operations, structure and building monitoring, horticulture and agriculture, etc, as the WSNs can be organized in disappeared aggressive situation. The execution for WSN hence expanding exponentially and in coming years, WSN would be a vivacious share of humanoid lives. The critical issue of deploying WSN is a security features as sensor nodes that intellect and take serious records. In this review paper, the authors recommend the expressive assessment is the issues of deploying security features in wireless sensor networks. Verification , authentication and validation is confirming that it will secure wireless sensor networks nodes, group cluster heads and base stations before allowing a undemonstrative support or see-through figures.

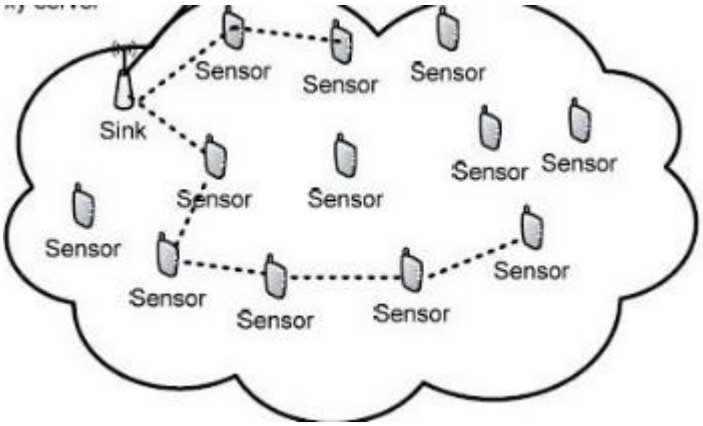
Keywords— wireless sensor network, security, internet of things, authentication, network, internet.

I. INTRODUCTION

Wireless Sensor Network is a collection of the base station and multiple sensor nodes, which are deployed to sense and collect different types of data. Sensor nodes consist various units like sensors, micro-controller, memory, microprocessor, antenna, battery, etc[1]. Sensor unit sense and collects data like humidity, pulse, temperature, pressure, etc. These nodes usually tend to face some serious problems like resource constraints and energy constraints due to deployment conditions and their size. The WSN is usually deployed, where the wired deployment is not possible due to various reasons like harsh hostile environmental conditions, emergencies, secrecy, etc. The major deployment areas of WSN are troops tracking, healthcare, [2] border monitoring, forest fire detection, earthquake detection, rescue operations, etc. Nodes anchored in such locations, over a period of time, may not be accessible physically after their post-deployment to repair its internal components which are a big hurdle to maintain wireless sensor network. Hence there is a need to have an efficient security mechanism to transmit the data for a large period of time, to protect the nodes and other components of net work from unauthorised acess.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Various improvements in the space of Wireless Communication and the electronics Science has given the improvement of low-power, low production cost, small sensor nodes.



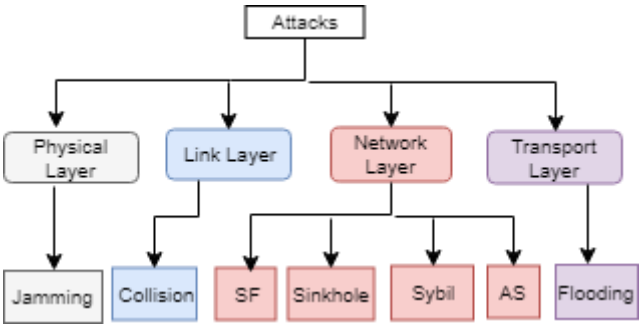
In WSN networks, most of the information that was sensed will be broadcasted. As a result, there is a possibility of data alteration and intrusion into the network or sensor nodes by a unauthorised person. In order to overcome these problems security must be established in network. This review paper present different actualities of different stabbings in Wireless Sensor Networks and its action taking methods against the stabbings, various security threats, security fears and security contracts, as well as the associated research effort done in such domain so far that linked with the area of deploying security in Wireless Sensor Networks

II. ATTACKS IN WSN

Nodes attacks can be characterized on the root of different network layers mentioned in Network Model commonly referred as physical layer, packet data link layer, Routing Network and last layer of the model is network data transport layer. The attacks involved in the WSN are listed and discussed underneath: -

Sinkhole-In this type of attack, the attacker makes a covert node that looks normal and attractive when compared to the normal nodes in the network. Due to this the neighbour surrounded nodes choses the covert node to send the data

Sybil-This is a kind of clone attack, in which the nodes have more than one identity. Attacker uses this and uses those clones to leak data and replaces the fake data as well.



Acknowledgment spoofing (AS) - In this attack generally, the attacking node sends false or fake information to its neighbour nodes. For instance, claiming that sensor node is deceased when it is actually active. The type of this attack is called as Acknowledgement Spoofing.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Selective Forwarding (SF)- Generally the nodes uses multi-hop routing techniques to transmit the data to the Base station. An attacker can make corrupt network nodes that bead vital grave information purposefully while transmitting the data packets. This can be countered to certain extent by implementing multi path routing.

Collision- When a node transmits data on some frequency, the attacker makes another node to transmit at same frequency. As a result packet collides with each other and collision happens.it is most prominent at link level.

III. Security Requirements

Generally security in WSN means the network has to provide confidentiality, availability, and integrity.

Confidentiality: It ensures to maintain the secrecy between nodes while they transmit the information, by restraining the information access only to granted public.

Integrity: It should give assurance to sensor network that data will not be altered while its transmission from one end to another end.

Availability: the network should provide services regardless of time, at whenever the authorised users needs them.

As WSNs are networks, where time critical information sharing was carried out all the time, security requirements are sophisticated, it needs further security necessities.

These can be categorised into three groups:

Data level requirements:

Recent Data - To guarantee that the information generated is topical and not transformed. In other Comes from a real sender.

- words, the data should be recent or fresh not to be modified.

Access Level Requirements:

- Authentication and Validation - Verification of the acknowledged information whether it was received from a actual sender or not
- Permission – it should ensure that lone allowed devices have permitted to access wireless sensor network.

Network level requirements:

- Strength - To assurance that the wireless sensor network is clever to job and assist the drive if the series of sensor nodes raises or the circumstance of few sensor nodes gets compromised.

IV. Authentication

Data Authentication: In a wireless sensor network, an enemy can without much of a stretch infuse messages. The recipient needs to ensure that the information utilized as a part of any basic leadership process starts from the true blue source.

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Information confirmation keeps unapproved parties from partaking in the system and true blue elements ought to have the capacity to identify messages from unapproved substances and reject them. Measures for ensuring uprightness are viewed as important to distinguish message modification and to dismiss infused message. Media access controls are used for granting access to public in the symmetric key cryptography technique. The sender and recipient share a private key to process a media access control of all conveyed information. When a correct media access message attains, the receiver already identifies that it is more frequently than not directed by the original sender. In universal society key cryptography, system generated marks are used to screen a message as an authentication and verification method. A system generated mark is a scientific project to demonstrate the validity of an progressive message, statement or document. A substantial unconventional mark gives recipient a reason to believe that a acknowledged sender has sent or transmit the information message, and that the information was not altered during the entire transmission. Computerized signature includes substantially more calculation overhead in marking, unscrambling, checking and encoding activities than techniques used in symmetric cryptography.

Node Authentication: Authentication is required for data exchange procedure and also for network administrative works in WSNs like the addition of new node to the networks. Several researchers have focused on node authentication before the nodes join the WSN such as protocol described by Manivannan *et al*. [2]. This protocol is in view of consistency conditions and number hypothesis ideas to accomplish secure confirmation among hubs in WSNs. Most research extends on the hub validation and key appropriation accept WSN as a static domain. Along these lines, they just spotlight on the effective introductory validation and key setup. However, considering the mobility of the nodes in WSN, other schemes have been proposed to take into consideration the mobility of nodes such as scheme presented by Han *et al.* [3]. The [4] DNA conspire utilizes geographic area and trust relationship among neighboring sensor hubs to verify the character of sensor hubs.

User Authentication: User authentication is a mean of distinguishing the client and confirming that the client is permitted to get to some confined administrations. Client confirmation implies setting up a connection between the client and some personality. A personality is the singularity property of a client which in a perfect world can't be produced or duplicated. By and by, personalities are actualized by things which clients know (passwords), have (mystery keys or security tokens) or properties which they have (biometrics).

In WSN, access to the gathered information will by and large not be free since organization of WSNs initiates a few expenses of sending. This implies the arrangement offices will make the detected

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

information accessible just to specific individuals, for the most part the individuals who pay for getting the administration. For this situation, a WSN must have the capacity to recognize honest to goodness clients from the ill-conceived ones. In confirmation, a client sends his ID (e.g., name, IP address) and evidence of his personality to a sensor so the sensor can choose whether or not the character is legitimate and in truth has a place with the client of that name. Upon fruitful validation, the sensor approves the client who is conceded access to the information.

Verification Factors: The present verification and authentication procedures comprises three elementary “factors”:

- Somewhat the handler distinguishes (e.g., login password, Pattern Indentification, passphrases);
- Somewhat the handler has (e.g., passkeys, symbols, identification id, tokens, biometric or smart cards);
- Somewhat the handler is (e.g., biometric features, DNA, facial scan fingerprint scans, speech match, impression, eye retina scan).

V. LITERATURE REVIEW

Benenson et al. [2] propose a client confirmation plot in view of open key cryptography, which tends to the issue of hub catch assaults. The plan keeps unapproved clients from getting to information gathered by sensor hub even within the sight of hub catch assaults. The plan is t-out-in, i.e. as the amount of trafficked off, sensor hub has not plentiful as t (where t is less than n, besides n is the amount of sensor hubs in the communication possibility of the patron) hub stays secure. The procedure of verification is as per the following. To begin with, the client communicates his personality and his testament as a demand. At that point, every hub in client's closeness sends a nonce to the client. This last signs the nonce and sends it back to the previous, which checks the legitimacy of the marked hash utilizing client's authentication and people in general key of the confirmation expert. Client must be validated by m hubs with a specific end goal to be permitted to post questions in the system. Be that as it may, this plan shows a few downsides. In the first place, it requires that each match of hub shares a mystery key, which prompts high storage room requires and thus does not scale well. Second, the plan permits questioning just a single hub of the WSN. This hub must be distinguished by hubs in client's nearness. The best approach to recognize the objective hub isn't introduced in Benenson's answer, and this fundamentally requires every hub knows about the whole system. Third, the plan does not address the situation where the hub in charge of preparing the inquiry is traded off and in this way can send false data..

Jiang et al. [3] proposed a conveyed client confirmation conspire in view of the Self-Certified

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

Keys cryptosystem (SCK), which they adjusted to utilize Elliptic Curve Cryptography (ECC). In their plan, they expect the nearness of a Key Distribution Center (KDC), which is in charge of creating a private/open key for every sensor hub in the system and for clients. At the point when a client wishes to obtain entrance, he first communicates his character and the parameter R (used to register general society key of client). At that point, every hub getting this entrance ask for figures the pairwise key, imparted to the client, utilizing ECC and afterward send a scrambled nonce to the client. This last should decode k nonces (where k is the limit) with a specific end goal to access arrange.

Wong et al. [5] proposed a productive client verification conspire. It depends on client's secret key and uses cryptographic hash work. It has security imperfections like numerous signed in clients with the same login-Id risk in which if an assailant has a substantial client's secret word, he/she can login to the sensor organize. It additionally experiences stolen-verifier assault as both GW-hub and login-hub keeps the look-into table of enlisted client's mystery data.

Jiang et al. [6] proposed an appropriated client confirmation plot in WSN. It depends on self-confirmed cryptosystem (SCK) which is adjusted to utilize ECC to set up pairwise enters in sensor systems. Here the hubs which are in the transmission scope of client, act cooperatively to see if the client is permitted to get to the sensor organize or not. The downside with this plan is that every hub which gets the entrance ask for from the client needs to process a pairwise key which will be imparted to the client. It additionally utilizes a scrambled nonce utilizing ECC, which is a costly undertaking for sensor hub.

Wuu Yang et al. [7] devised a dynamic patron authentication conspire for isolated sensor establish in view of elliptic bend crypto-framework with self-endorsements. In this plan, KDC (key appropriation focus) is in charge of initialing framework parameters, creating character, producing private/open key-match and circulating the authentication to every client and every sensor hub. The issue is the two clients and sensor hubs need to accumulate a great deal of arguments. At this point, the user’s behavior is established via the wireless sensor hub by read-through the mark employing elliptic curve, which is an excessive task. The method moreover practices DoS attack. At this time, the sender transmits unenforceable authentications or mark to the sensor hub the aggressor could deplete the remembrance on the hub or making the hub approaching up short on vitality.

Sain et al. [8] implemented a talented dual-factor patron verification structure for distant sensor systems, that be subject on undisclosed term and brilliant card, and it utilizes one-way hash work. This plan gives shared validation and gives client office to change watchword at require. Be that as it

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

may, the issue here is, it doesn't limit special insider assault as the secret word is sent in flat material to the base station hub. This mechanism furthermore practices the organization issue as this mechanism employs the period stamp for preserving a planned detachment from repetition outbreak.

Gurtov et al. [9] reveals that security imperfections, hasn't capable for honest wireless sensor network. Wireless sensor networks for isolated sensors are utilized for some constant applications. Client confirmation is a vital security benefit for WSNs to guarantee just authentic clients can get to the sensor information inside the system. In 2012, Yoo et. al implemented a wireless sensor security execution model suggests the client validation plot for WSNs, which is an improvement of existing plans. What's more, this paper proposes another solid validation conspire with client security for wireless sensor networks. The recommended model not just achieves closeparty common validation (exits amongst the patron and the wireless sensor hub) moreover cliques a energetic conference key. The devised conspire jam the safety highlights of author model and other prevailing strategies that provides supplementary down to earth security administrations. Moreover, proficiency of the devised plot is more appropriate for factual wireless sensor networks applications.

Rodrigues et al. [10] implemented a handler substantiation routing protocol in wireless sensor networks. Lately, remote sensor systems (WSNs) have been broadly utilized as a part of various areas. For example, WSNs can be sent in uncertain and unattended situations. In such manner, client verification is a basic issue for WSNs. The proposed convention is assessed and contrasted and the past plans.

Koubaa et al. [11] implemented a inconsequential user authentication conspire adjusted to wireless sensor networks that provides collective authentication and assembly key assertion. Client confirmation in established systems is profoundly tended to, however few outcomes are identified with Wireless Sensor Networks (WSNs). What's more, the proposed plans don't give common verification or session key mediating amid the wireless sensor network server and the patron. The proposed plot permits a client outfitted with cell phone (ordinarily PDA) to confirm himself before accessing the wireless sensor networks. The proposal is carried out on dual sides; the customer end controlling the cell phone of the customer and the server end spoke to the controller of the wireless sensor network. A safety examination of model exhibited and the model establishes his forte in contrast to established kinds of assaults. Proposed model additionally actualized genuine stage of sensor hubs. Usage reveals that author’s model is frivolous or trivial as the model entails roughly just is to perform its complete execution. What's more, the authors have completed an inspection amongst their model and the existing

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

model in view of their safety assets. Furthermore authors revealed that their devised model outflanks the current ones as far as secrecy, trustworthiness, shared confirmation and session key age with a lightweight calculation overhead.

Fouchal et al. [12] proposed a conveyed arrangement ready to guarantee validation of hubs whenever without having any on-line access to a declaration expert. Safety is essential for remote sensor systems (WSN) installed in hostile situations as many kinds of assaults may diminish the conviction in any wireless sensor network's worldwide activity. Numerous arrangements have been devised to protect correspondences for wireless sensor networks and the greater part between the wireless sensor network hinge on a brought together segment which carries on as a declaration specialist. Every hub would be furnished with a TP module. The TP module is referred as trusted platform module that can accumulate symmetric keys with safety. Every hub would take its individual open key and secret key syndicate in the trusted platform module with declaration of general population key. The authentication is delivered disconnected during the installing up the hub. At the point when a hub speaks with alternative, the hub needs to verify the communication with its individual particular secret key (complete safely by the trusted platform module) and directs the communication, the mark and testament of general society key. Assessment of arrangement has been finished utilizing recreation and the overhead included by coordinating verification does not surpass 15% of vitality utilization.

Wei et al. [13] proposed and implemented one approach of common validation plot with key assention for remote sensor arrange, which is noteworthy to security provisioning in remote sensor connect with asset constraints. Security assumes a particularly essential part for use of remote sensor arrange because of the powerlessness of system. This paper likewise talked about new sensor hub security join process in the system. In light of the arrangement idea, the proposed conspire does not require open keys for sensor hubs with the end goal that the extra cost for declarations can be lessened. At last, test comes about demonstrate that these security strategies might be utilized to understand the security and dependability of the remote sensor systems.

Yoo et al. [14] portray and cryptanalyze past everything in client verification to delineate their susceptibilities and safety imperfections. The employments of remote sensor systems have expanded to be pertinent in a wide range of regions, for example, armed forces applications, environment and security applications. The remote sensor system applications frequently incorporate the direction of classified data by creating the threat of safety, a standout amongst the maximum essential viewpoints to contemplate. In this

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

viewpoint, a client verification component enables just real clients to get to the system information ends up basic for keeping up the classification and respectability of the system data. This paper likewise proposes a vigorous client validation conspire that explains the distinguished constraints. Also, depict how the proposed convention is more appropriate for a safe sensor organize usage by investigation regarding security and execution.

Nam et al. [16] implement a safety demonstrate for the inspection of SUA wireless sensor network conspires expanding generally acknowledged prototypical of BPR. A shrewd card-based client verification conspire for remote sensor systems (to put it plainly, SUA wireless sensor network plan) intended to confine admittance to wireless sensor information just to clients. The clients works under the govern of keencard and the connecting private key. While countless wireless sensor network schemes have been suggested as of late, their proposed safety properties need prescribed descriptions and confirmations in generally acknowledged prototype. The initial result is that SUA wireless sensor network plans unreliable contrary to different assaults has multiplied. Proposed model gives formal meanings of validated key trade and client secrecy while catching side-channel assaults, and also other basic assaults. Creators furthermore suggest another SUA wireless sensor network plan in the view of elliptic curve cryptography, and reveal its safety assets in their broadened show. The finest in their perception, the anticipated conspire is main SUA wireless sensor network plot that provably accomplishes together confirmed key trade with client secrecy. This plan is additionally computationally focused with other ECC-based plans.

Abduvaliev et al. [17] propose straightforward hash oriented communication validation & verification with trustworthiness cypher calculation for remote device systems. Implemented scheme utilizes presegment anonymous symmetric key that is attained from elliptic curve diffie hellmann (ECDH) key trade scheme, oriented on transformed “SHA-1 (mSHA-1)” hash job that registers communication validation cypher for assumed communication. Creator recommend dual situations trusting upon size of the system, and furthermore break down safety of the devised calculation. That’ calculation gives altogether uprightness with credibility of a communication just with a sole hash esteem.

V. CONCLUSION

In WSN networks, most of the information that was sensed will be broadcasted. As a result, there is a possibility of data alteration and intrusion into the network or sensor nodes by a unauthorised person. In order to overcome these problems security must be established in network. The above review paper reveals realities of diverse assaults in wireless sensor networks and its action taken against the

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

diverse assaults, different safety concerns , safety resolutions, moreover associated research work completed as such exits in the domain of security and safety in wireless sensor networks.

REFERENCES

[1] Qinghan Xiao, "A Biometric Authentication Approach for High Security Ad-Hoc Networks", IEEE, 2004, pp. 250-256.

[2] D. Manivannan, B. Vijayalakshmi, P. Neelamegam, "An efficient authentication protocol based on congruence for Wireless Sensor networks", International Conference on Recent Trends in Information Technology, Chennai, India, 2011, pp. 549-553.

[3] K. Han I, K. Kim I, T. Shon, "Untraceable Mobile Node Authentication in WSN", Sensors, Vol. 10, 2010, pp. 4410-4429.

[4] Q. Zhang, X. Zhou, F. Yang, "Distributed Node Authentication in Wireless Sensor Networks", International Conference on Wireless Communications, Networking and Mobile Computing, Beijing, China, 2009, pp. 1-4.

[5] Kirk HM Wong, Yuan Zheng, Jiannong Cao, and Shengwei Wang. A dynamic user authentication scheme for wireless sensor networks. In Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on, volume 1, pages 8–pp. IEEE, 2006.

[6] Canming Jiang, Bao Li, and Haixia Xu. An efficient scheme for user authentication in wireless sensor networks. In Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on, volume 1, pages 438–442. IEEE, 2007.

[7] Huei-Ru Tseng, Rong-Hong Jan, and Wuu Yang. A robust user authentication scheme with self-certificates for wireless sensor networks. Security and Communication Networks, 4(8):815–824, 2011.

[8] Pardeep Kumar, Mangal Sain, and Hoon Jae Lee. An efficient two-factor user authentication framework for wireless sensor networks. In Advanced Communication Technology (ICACT), 2011 13th International Conference on, pages 574–578. IEEE, 2011.

[9] Pardeep Kumar, Andrei Gurtov, Mika Ylianttila, Sang-Gon Lee, HoonJae Lee, "A Strong Authentication Scheme with User Privacy for Wireless Sensor Networks", ETRI Journal, Vol. 35, No. 5, October 2013, pp. 889-899.

[10] Binod Vaidya, Jorge Sá Silva, Joel J. P. C. Rodrigues, "Robust Dynamic User Authentication Scheme for Wireless Sensor Networks", 2010.

[11] Omar Cheikhrouhou, Anis Koubaa, Manel Boujelben, Mohamed Abid, "A Lightweight User Authentication Scheme for Wireless Sensor Networks".

ISSN: 0971-1260
Vol-22-Issue-17-September-2019

[12] Hacène Fouchal, Javier Biesa, Elena Romero, Alvaro Araujo, Octavio Nieto Taladrez, "A Security Scheme for Wireless Sensor Networks", IEEE, 2016.

[13] Min Wei, Keecheon Kim, Ping Wang, "Research on A Mutual Authentication Scheme for Wireless Sensor Networks", IEEE, 2012, pp. 523-528.

[14] Sang Guun Yoo, Keun Young Park, Juho Kim, "A Security-Performance-Balanced User Authentication Scheme for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, 2012, pp. 1-11.

[15] Joel Joy Manjaly, J Sandeep, "An Authentication Protocol for Clustered Wireless Sensor Networks", International Journal of Advanced Research in Computer Science, Vol. 8, No. 3, 2017, pp. 198-203.

[16] Junghyun Nam, Moonseong Kim, Juryon Paik, Youngsook Lee, Dongho Won, "A Provably-Secure ECC-Based Authentication Scheme for Wireless Sensor Networks", Sensors, 2014, pp. 21023-21044.

[17] Abror Abduvaliev, Sungyoung Lee, Young-Koo Lee, "Simple Hash Based Message Authentication Scheme for Wireless Sensor Networks".