



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 Issue: II Month of publication: February 2021

DOI: <https://doi.org/10.22214/ijraset.2021.33005>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Survey on Advanced Data Communication Using Protocol

Shahul Hameed A¹, Dr. A. Shaji George², Bashiru Aremu³

¹Ph.D. Research Scholar, Department of Information and Communication Technology, Crown University, Int'l. Chartered Inc. (CUICI) Argentina Campus, South America.

²Professor, Department of Information and Communication Technology, Crown University, Int'l. Chartered Inc. (CUICI) Argentina Campus, South America.

³Vice Chancellor, Crown University, Int'l. Chartered Inc. (CUICI) Argentina Campus, South America.

Abstract: *There are various remote sensor organization (WSN) applications being created day to day. These applications range from straightforward natural checking, for example, gathering temperatures in an agrarian ranch to complex applications, for example, observing front lines. As the applications increment so are the assaults. Subsequently, a few security conventions have been acquainted with be utilized with the various applications which have changing security necessities; this infers that the decision for the WSNs application ought to be very much thought of. This paper talks about the remote sensor organization security prerequisites, the most well-known assaults and the most mainstream conventions utilized with WSNs. Center is likewise given to the qualities and restrictions of WSN security conventions to empower planners of the WSNs pick the correct convention for their applications.*

Keywords: WSN, Access control, Framework, Private key, Cloud computing

I. INTRODUCTION

A wireless sensor network (WSNs) contains numerous indistinguishable hubs with restricted assets. Sensor hubs impart remotely and they brilliantly measure flags and send information over the organizations. These hubs are typically spread over the entire organization region for observing, information assortment, handling, and sending to a base station to handle further (Sharma, Chaba and Singh, 2010). The Sensors are little in size, restricted in terms of intensity and their expense is regularly low.

Sensors have the accompanying capacities:

correspondence is over short distances, they can detect or peruse information from the climate, furthermore, their information handling capacity is restricted. Regularly sensor works at 2.4 GHz recurrence, 250Kbps information rate, streak memory is 128KB, memory of 512KB for reason for recording estimations, they communicate powers going from 100uW and 1mW, and correspondence range is between 30m to 100m. Accordingly, the best plan thought ought to be energy proficiency of WSN conventions (Uluagac et al., 2008). The best test for WSNs are security issues, and for certain sensor networks applications, similar to medical care applications and military applications security turns out to be significantly more critical. These challenges are as per the following:

- i. It's hard to ensure remote correspondence since it is finished by broadcasting. Bundles can be infused, snooping is a probability, capture of moving information, and information sent can be modified effectively by enemies.
- ii. The WSNs might be introduced in conditions that are possibly shaky; where there is a chance for enemies to take on the appearance of approved hubs in the organization, and hubs taking can happen.
- iii. The WSNs are vulnerable to assaults of utilization of assets. Aggressors can squander network data transmission and often send bundles to debilitate a hub battery. Because of these elements, it's basic for the delicate computerized data to be safely sent over the sensor organizations.

II. SECURITY REQUIREMENTS

WSNs are utilized in bunches of utilizations with distinctive security prerequisites. E.g., an application for natural checking requests less security though; war zone checking applications requests high security levels. For natural checking applications in-network handling is indispensable to lessen the organization conflict (Ahmed, 2009). As indicated by Sharma, Chaba and Singh, 2010 the security prerequisites or administrations are for example, accessibility, approval, confirmation, privacy, uprightness, non-disavowal, information newness, vigor, self-association and time synchronization.

A. Accessibility

This is a security administration that verifies whether a given hub can use the assets and additionally if the organization is accessible to impart messages. The WSN can be imperiled if the sink (base station) or group head comes up short. Accordingly accessibility is significant for an organization to be operational (Padmavathi and Shanmugapriya, 2009). The accessibility security administration for WSNs has been taken a gander at top to bottom from the Denialof-Service (DoS) type assaults measurement in expansion, properties for interfacing WSNs as concerns accessibility has additionally been concentrated in extraordinary length (Uluagac et al., 2008).

B. Approval/Access control

This guarantees that lone approved clients and gadgets approach the WSN.

C. Confirmation

This security necessity guarantees that there is legitimate correspondence from an offered hub to another hub; this implies an untrusted hub can't imagine as a confided in hub (Rajkumar.et al., 2012.).

D. Secrecy

Secrecy is alluded to as the ability to conceal messages from any given foe (aggressor) to guarantee any message sent through the WSN is secret (Padmavathi and Shanmugapriya, 2009). In case an adversary, gets to the substance, he ought to not have the option to interpret the messages traded in the organization. To give a secret security administration to WSNs applications you require the utilization of cryptographic instruments, for example, encryption strategies. By and large, two sorts of encryption approaches are utilized;

- 1) Symmetric encryption
- 2) Unbalanced encryption.

Symmetric encryption utilizes the indistinguishable key at both the sender and collector hubs to encode and unscramble the data from plain content to encode text and the other way around. While lopsided key based encryption, utilizes different keys, one public and the other private which are utilized to change over and recuperate the data (Uluagac et al., 2008).

There is no single encryption component that one can guarantee is superior to another as it is essentially an issue to do with size of the key and the computational exertion that can be used to break the encryption calculation.

Another feature to privacy research in WSNs is on issue of planning effective key the board plans. The keys must continuously be accessible to all the hubs imparting and this guarantees security of channels is kept up (Uluagac et al., 2008). The way toward overseeing keys includes two essential advances;

- a) Key age
- b) Keys appropriation

This cycle is set off by keying occasions like organization assault. Nonetheless, it is anything but a straightforward undertaking and in various applications it very well might be overpowering activity to go to each and every sensor considering their numerous numbers and updating of their keys, for-example underwater sensor applications. Therefore, management of keys intelligently is essential for WSNs (Uluagac et al., 2008).

E. Integrity

Trustworthiness is essentially affirmation of a message not being changed, altered or then again changed (Padmavathi and Shanmugapriya, 2009). On the message content a substance digest is added to give uprightness of content traded. On receipt of message by the getting hub content condensation is checked to affirm that substance digest processed and gotten digest are equivalent. When affirmed to be equivalent or same at that point it's treated as a genuine message.

Hashing calculations are utilized to make content condensations (Uluagac et al., 2008). There are a few calculations for hashing accessible and these calculations don't as a rule require the keys presence except if planned explicitly to work with keyed-hashing for example Keyed-Hashing for message Validation Code (HMAC) and Cipherbased Message Authentication Code (CMAC) (Uluagac et al., 2008). Respectability administration checks information lifelessness since a few choices for certain applications relies upon whether the information is later or it's not. For-instance, waters of a given region can be ensured with sinks exploded mines. Message newness and its exact planning from the sensor hubs in this sort of application are basic (Uluagac et al., 2008).

Honesty administration likewise is intended to give a component for recuperation from any substance that has been changed (Uluagac et al., 2008).

F. Non-repudiation

Non-repudiation security service ensures that a node cannot deny the messages it has sent (Rajkumar et al., 2012). To offer non-repudiation service digital signature scheme (DSS), which utilizes encryption methods, can be used. DSS can use either symmetric or asymmetric encryptions (Uluagac et al., 2008).

When you use symmetric encryption the WSN may be in danger of another sensor masquerading as the sensor's original signature. On the other hand, using asymmetric encryption may be expensive. Basically non-repudiation service facilitates the approval by another entity for messages sent or received in WSNs. Therefore, a legitimate node, such as the base station (sink) can offer the service (Uluagac et al., 2008).

G. Data Freshness

This guarantees that the data over the WSN is current and not replicated

H. Robustness

This guarantees that in the event of some nodes being compromised, the WSN continues to operate.

I. Self-organization

This ensures that the sensor nodes are independent and can be flexible in the event of adding new nodes or some nodes fail. WSNs are basically ad hoc networks; this characteristic makes it prone to security issues. Therefore, in the circumstance self-organization and self-healing is impossible then the damage could be overwhelming.

J. Time Synchronization

WSNs applications rely on time synchronization for purposes such as; power conservation, packets end-to-end delay computation, and group synchronization for tracking applications.

K. Secure Localization

This is a requirement for the sensor nodes to be able to securely identify its location (Pathak & Quaz, 2017). Attacks on Wireless Sensor Networks Wireless sensor networks attacks are categorized by different authors as follows;

- 1) Active attacks and passive attacks. The active attacks modify data and include Blackhole, Sybil, HELLO Flood attack, denial of service and wormhole attack. The passive attacks are such as; attacks against privacy, eavesdropping and traffic analysis (Padmavathi & Shanmugapriya, 2009).
- 2) According to Sunitha & Chandrakanth (2012), wireless sensor networks attacks are in three categories;
 - a) Secrecy and authentication attacks – These attacks are such as spoofing, eavesdropping, and packet replay attacks.
 - b) Attacks on network availability These attacks are also known as denial-of-service (DoS) attacks.
 - c) Stealthy attack against service integrity – The attacker makes the WSN acknowledge a false data value. E.g. through injection of false data value.
- 3) Attacks against security mechanism and attacks against routing mechanisms (Pathan, Lee & Hong, 2006)

The major WSN attacks are

- Wormhole attack The attacker near a base station tunnels the traffic to a low latency link thus disrupting the traffic
- Hello flood attack This attack happens when assumption is made that the node broadcasting HELLO packets is a genuine neighbor. This can cause a large number of nodes to attempt to use this route, thus sending packets into oblivion.
- Blackhole attack This attack is when all packets are dropped, meaning none is transmitted.
- Sinkhole attack This kind of attack occurs when a malicious node attracts maximum traffic through it
- Denial of service attack (DoS) The attacker ensures that the legitimate users don't gain access
- Sybil attack This is when a node masquerades with multiple identities in the network.
- Attacks on information in transit
- Selective forwarding This attack makes some packets to be dropped and others are transmitted
- Spoofing

III. SECURITY CHALLENGES IN WSN

The universal approach for defense against cyber-attacks is cryptography, but there exists challenges in keeping required level of security and safety of critical data transmitted over wireless sensor network. WSN has myriad of inherent challenges when compared to the conventional computer networks. The table below compares the WSN and the traditional networks.

A. Remote Sensor Networks Security

Conventions Security convention is characterized as a bunch of rules that decide how the connection between peer cycles to make accessible guaranteed security administration (Aseri and Singla, 2011). A number of security conventions have been proposed to date, and the most famous for WSN are talked about in this part.

- 1) *SPINS*: Twists was proposed by Perrig et al., 2002, what's more, it's an assortment of security conventions upgraded for sensor organizations. Twists has two secure structure hinders explicitly Secure Network Encryption Protocol (SNEP) and u TESLA. SNEP gives information verification for two gatherings, secrecy of information, and newness of information while u TESLA verifies communicates. Restricted capacity obstacle is accomplished by conventions through the reuse of code for all crypto natives, for example, message validation code, encryption, and hash irregular number generator. Moreover, to lessening the correspondence overhead, it divides the basic state among correspondence parties. Semantic security is accomplished through SNEP by joining counter in both sender and recipient closes. It's critical to take note of that the counter isn't fused with the message in order to decrease the information transmission rate (Ahmed, 2009). SNEP bolsters just base-to-hub correspondence and the other way around while uTESLA gives validated transmission. Customarily to confirm communicates you require uneven keys to validate the beginning parcels, however u TESLA utilizes symmetric key to furnish security with symmetric keys exposure deferred. Shockingly with a organization of numerous hubs synchronization is a challenge (Ahmed, 2009).
- 2) *TINYSEC*: TinySec is a connection layer security conventions for Remote sensor organizations (WSNs), and its primary distinction with the SPINS is that it doesn't utilize counters. The arrangement of uninvolved correspondence (in-network preparing) is finished by Link layer security among neighborhood hubs to kill interchanges that are covering with the sink (base station) (Ahmed, 2009). Karlof et al., 2004 planned TinySec to supplant the inadequate Sensor Network Encryption Protocol (SNEP), called TinySec. TinySec is interface layer security engineering for WSNs and it offers security administrations, for example, access control, secrecy, and message uprightness
- 3) *Link-layer security protocol (LLSP)*: Lighfoot et al., 2009; designed a Link-Layer Protocol (LLSP) and the goal was to develop a protocol with low energy requirements as compared to Tiny Sec. LLSP ensures message confidentiality, message authentication, replay protection and access control. LLSP supports early rejection capability in addition, it has low performance overhead. However maintaining a large network is difficult within node counter due to that it has low scalability.
- 4) *Light weight security protocol (LiSP)*: LiSP is a lightweight security mechanism that supports key renewability and puts into balance the need for security and consumption of resources. LiSP from time to time renews the shared key to solve the problem of reuse of key stream-reuse and maximize energy efficiency and scalability. LiSP also supports distribution of keys which is reliable (Park & Shin, 2004). LiSP is efficient in terms of energy and is robust to denial of service (DoS) attacks, since it doesn't require retransmitting or any control packets. LiSP has a joint authentication and recovery algorithm for rekeying, where Key -Server (KS) from time to time a new key is broadcast before it's used for encryption and decryption. The key received is authenticated by client node and then recovers all keys that have been missing (Park & Shin, 2004). The goal of LiSP is to offer a lightweight security solution for a large-scale network of resource-limited sensor devices. LiSP divides the whole network into clusters and selects a Group-head (GH) for each of them to offer scalability for a large number of sensors (Park & Shin, 2004).
- 5) *Location aware end-to-end security (LEDS)*: LEDS offers location aware end-to-end security. Several sensing nodes endorse genuine event reports in LEDS and are encrypted with a unique secret key which is shared between the sink and event sensing nodes. LEDS provides end-to-end authentication and en-route filtering capability to deal with the recognized attacks for injection of data. If there are no more than a given stated number of compromised nodes in each single area of interest, LEDS assures that a fake or false data report from a given cell can be filtered by genuine in between sink or the nodes (Ren, Lou, & Zhang, 2008). LEDS provides location aware key management. LEDS can be used in both small and large networks and the key numbers increases with size of the cell. In addition, LEDS doesn't support dynamic topology. LEDS puts the network into several cell regions and when an event occurs in a given region, the event should be sensed by several nodes (Ahmed, 2009). Data availability is assured by LEDS because it deals with both report disrupting attack and selective forwarding attack at the same time. Wireless links are broadcast in nature and so LEDS adopts one node to many nodes data forwarding approach,

this ensures LEDS reports are authenticated by several next-hop nodes separately. This means that no reports disappear due to being dropped by a single node. (Devi et al., 2011) LEDS ensures a very high level of security without considering the costs for communication and computing in addition LEDS provides data confidentiality and node capture attacks to a reasonable level (Ahmed, 2009).

IV. CONCLUSION

In the face of myriad of challenges facing WSNs architects of WSNs are confronted with hard decision of security convention to actualize. This paper has summed up the distinctive security prerequisites for WSNs, the security conventions and the security prerequisites they accomplish and of significance an outline has been given to show the qualities and constraints of every one of the security convention. This will go in convenient to help facilitate the cycle of decision of security convention to be actualized in different applications.

REFERENCES

- [1] Aseri, T. C., & Singla, N. (2011). Enhanced Security Protocol in Wireless Sensor Networks. *International Journal of Computers Communications & Control*, 6(2), 214-221.
- [2] Bhalla, M., Pandey, N., & Kumar, B. (2015, October). Security protocols for wireless sensor networks. In *Green Computing and Internet of Things (ICGIoT), 2015 International Conference on* (pp. 1005-1009). IEEE.
- [3] Boyle, D., & Newe, T. (2007, March). Security protocols for use with wireless sensor networks: A survey of security architectures. In *Wireless and Mobile Communications, 2007.ICWMC'07. Third International Conference on* (pp. 54-54). IEEE.
- [4] Devi, S. A., Babu, R. V., & Rao, B. S. (2011). A new approach for evolution of end to end security in wireless sensor network. *International Journal on Computer Science and Engineering*, 3(6), 2531-2543.
- [5] Dutta, R., Gupta, S., & Paul, D. (2014, December). Energy efficient modified spin protocol with high security in wireless sensor networks using tossim. In *Parallel, Distributed and Grid Computing (PDGC), 2014 International Conference on* (pp. 290- 294). IEEE.
- [6] Karlof, C., Sastry, N., & Wagner, D. (2004, November). TinySec: a link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems* (pp. 162-175). ACM.
- [7] Lighfoot, L.E., Jian R. & Tongtong L. (2009). An Energy Efficient Link-Layer Security Protocol for Wireless Sensor Networks. *IEEE EIT Proceedings* (pp 233-238).
- [8] Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *arXiv preprint arXiv: 0909.0576*.
- [9] Park, T., & Shin, K. G. (2004). LiSP: A lightweight security protocol for wireless sensor networks. *ACM Transactions on Embedded Computing Systems (TECS)*, 3(3), 634-660.
- [10] Pathak, P. & Quaz, M.A. (2017), Issues, Challenges and Solution for Security in Wireless Sensor Networks: A Review *International Journal of Electrical, Electronics ISSN No. (Online): 2277-2626 and Computer Engineering* 6(1).
- [11] Pathan, A. S. K., Lee, H. W., & Hong, C. S. (2006, February). Security in wireless sensor networks: issues and challenges. In *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference (Vol. 2, pp. 6-pp)*. IEEE.
- [12] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. *Wireless networks*, 8(5), 521-534.
- [13] Ren, K., Lou, W., & Zhang, Y. (2008). LEDS: Providing location aware end-to-end data security in wireless sensor networks. *IEEE Transactions on Mobile Computing*, 7(5), 585-598.
- [14] Sharma, R., Chaba, Y., & Singh, Y. (2010). Analysis of security protocols in wireless sensor network. *International journal of advanced networking and applications*, 2(3), 707-713.
- [15] Sunitha, K., & Chandrakanth, H. (2012). A survey on security attacks in wireless sensor network. *International Journal of Engineering Research and Applications (IJERA)*, 2(4), 1684-1691.
- [16] Uluagac, A. S., Lee, C. P., Beyah, R. A., & Copeland, J. A. (2008, October). Designing Secure Protocols for Wireless Sensor Networks. In *WASA* (pp. 503-514).
- [17] Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 2(4), 500-528.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)