COMPARATIVE STUDY ON VARIOUS AUTHENTICATION PROTOCOLS IN WIRELESS SENSOR NETWORK

SAROJA M,
B.Tech, Department of C.S.E
Mahaveer Institute of Science and Technology, Bandlaguda,
Hyderabad, T.S,

Abstract:

Remote sensor organizations (WSNs) comprise of lightweight gadgets with minimal effort, low force, and short-went remote correspondence. The sensors can speak with one another to shape an organization. In WSNs, broadcast transmission is generally utilized alongside the greatest utilization of remote organizations and their applications. Thus, it has gotten significant to confirm communicated messages. Key administration is likewise a functioning examination subject in WSNs. A few key administration plans have been presented, and their advantages are not perceived in a particular WSN application. Security administrations are crucial for guaranteeing the trustworthiness, validness, and secrecy of the basic data. Thusly, the validation instruments are needed to help these security administrations and to be versatile to unmistakable assaults. Different validation conventions, for example, key administration conventions, lightweight verification conventions, and broadcast confirmation conventions are thought about and dissected for all safe transmission applications. The significant objective of this study is to look at and discover the fitting convention for additional examination. Additionally, the correlations between different verification strategies are likewise shown.

Keywords:

Wireless sensor networks (WSNs), authentication techniques, Security services, network.

Introduction:

Remote sensor organizations (WSNs) are quickly filling in prevalence because of the ease answers for an assortment of difficulties in reality. WSN has no foundation support, is immediately sent in an area with a few minimal effort sensor hubs, is utilized for observing the climate, and is inflexible to keep up its security. It contains colossal number of asset sensor hubs, which are spatially scattered in the unfriendly climate. The assignment of the sensor hubs is to detect the actual marvels from their nearby neighbors and interaction and move the detected information to the base stations. Multiloop correspondence is liked in WSN as the quantity of hubs is exceptionally enormous, and sensor hubs have limitations concerning power, calculation, correspondence, and capacity.

Security in WSN gets essential since the hubs after the organization can't be physically kept up and noticed. The present circumstance turns into a significant issue in WSN because of its organization of correspondence. The validation is given to the information that can be sent or gotten to by any hub in the organization. Likewise, it is basic to forestall and acquire the data from the unapproved clients. As new dangers and assault models are proposed, a few sorts of confirmation components have been presented in WSN security. Validation component can be separated dependent on the accompanying rules:

(i)authenticating unicast, multicast, or broadcast messages,

(ii)symmetric (shared key) or unbalanced (public key) cryptographic strategy,

(iii)static, portable, or the two parts of WSN.

Different explores have zeroed in on highlight point verification components, which confirm unicast messages in WSN. Notwithstanding being secure, unicast strategies can't be applied directly to either multicast or communicate messages. Broadcast messages are straight acquired from the dependable sources and can't be changed during transmission. The fundamental parts of a transmission verification measure are

(i)checking the source character from which the message starts,

(ii)confirming the message trustworthiness for guaranteeing the message creativity.

Also, it offers insurance against

(a) falsification,

(b) replay assaults, and

(c) pantomime,

which are principle highlights of the validation components. There are two validation instruments dependent on the cryptographic techniques as talked about above. It can either be a symmetric strategy or a deviated technique. The previous strategies utilize shared key cryptography, where both the sender and the collector utilize comparative key during the time spent validation and check. The last case utilizes public key cryptography, where the sender signs a message with the private key and the beneficiaries confirm it by the separate public key.

In this overview, different existing verification conventions in remote sensor networks are talked about. A rundown of significant issues and open exploration challenges are looked at and dissected. Also, a comprehensive review on the accessible conventions for verification in the remote sensor organizations and their applications is given. The study likewise contains the significant parts of looking at the conventions based on quality estimation on a case by case basis for validation components. The examination tables are accommodated dynamic on the most fitting conventions. It satisfies the prerequisites of the specific application situation. This paper surveys a few validation conventions in WSN and its significant commitments are recorded as follows:

(i)comparison of different validation conventions,

(ii)information around a few existing validation conventions,

(iii)analyses of different plans with various boundaries in the current systems.

Security Issues in Wireless Sensor Networks:

1. Threats/Attacks on Sensor Node Routing

Several WSN routing protocols are simple and are vulnerable to attacks from those works on routing in ad hoc networks. Most threats against WSNs fall into one of the following groups:

(i)spoofed, altered, or replayed routing information,

(ii)selective forwarding,

(iii)sinkhole attacks,

(iv)Sybil attacks,

(v)wormholes,

(vi)HELLO flood attacks,

(vii)acknowledgment spoofing.

1.1. Spoofed, Altered, or Replayed Routing Information

This attack targets the information of a routing exchanged between the nodes. Adversaries are able to establish routing loops, produce false messages, maximize end-to-end latency, and extend or reduce source routes, network partition, and more.

1.2. Selective Forwarding

In this threat, malicious nodes may decline to forward particular messages and basically drop them. It makes sure that the malicious nodes are not propagated further as it behaves like a black hole; further all the received messages are rejected. The selective forwarding attacks are normally more efficient as the attacker is explicitly involved in the path of a data flow.

1.3. Sinkhole Attacks

By establishing a metaphorical sinkhole with the adversary at the middle, the attacker's goal is to get all the traffic within certain area via a compromised node. With respect to the routing algorithm, this attack can function by making a compromised node appear attractive to the nearby nodes. Various protocols might try to check the route quality with end-to-end acknowledgements comprising the information of reliability or latency.

1.4. Sybil Attacks

In this attack, a single node offers several identities to the other nodes in the network. It can significantly minimize the effectiveness of the fault-tolerant systems. This attack also causes a significant attack to geographic routing protocols. By using this attack, an adversary can be in various places at once.

1.5. Wormholes

Type of attack	Layer	Security mechanism
Jamming	Physical	() Lower duty cycle () Spread-spectrum technique
Tampering	Physical	() Key management schemes
Collision	Data link	() Error correcting code
Exhaustion	Data link	() Rate limitation
Replayed routing information	Network	() Encryption techniques () Authentication schemes
Selective forwarding attack	Network	() Redundancy technique () Probing mechanism
Sybil attack	Network	() Authentication schemes
Sinkhole attack	Network	() Authentication schemes () Redundancy technique () Monitoring
Wormhole attack	Network	() Flexible route selection method
HELLO flood attack	Network	() 2-way authentication method () 3-way handshake method
Flooding attack	Transport	() Minimizing connection numbers () Client puzzles
Clone attack	Application	() Unique pairwise keys

In the wormhole attack, an adversary in one part of the network can receive messages over a low-latency link and replay them in distinct parts via a tunnel. This attack usually includes two detached malicious nodes, which collude to minimize their distance from each other by replaying packets.

1.6. HELLO Flood Attack

This attack is a novel attack introduced against sensor networks, where the nodes can be convinced by the adversary to trust that the adversary is its nearby neighbor. This can possibly transfer the fake information with high transmission power. Many packets request nodes to broadcast HELLO packets by assuming themselves as their neighbor nodes. A node thus reaching such a packet will assume that it is within the radio range of the sender.

1.7. Acknowledgment Spoofing

This attack has the objective of proving to the sender that a dead node is still alive or a weak link is strong enough. Herein, an adversary can eliminate information transmitting to these dead nodes or weak links. Also, an adversary can eavesdrop packets addressed to the other nodes and identify which nodes are dead or weak.

Table 1 describes several attacks present in the WSN and their corresponding security mechanisms.

Table 1 Several attacks and their corresponding security mechanisms in WSN.

Security Requirements and Challenges in WSNs:

WSNs percentage a few common functionalities with a regular laptop community as it's miles a unique sort of network. It also reveals numerous traits which might be precise to it. In WSNs, the maximum crucial requirements for safety [4] are listed as follows:

(i)data confidentiality: it guarantees that no messages inside the network are understood with the aid of the recipient. also, it offers privacy for wireless communication channels such as cellular codes, software data, and manage message so that overhearing is averted.

(ii)Availability: it ensures the provider provided either by using the whole WSN or via any a part of it.

(iii)Authentication: earlier than allowing a confined resource or revealing records, it authenticates the sensor nodes, cluster heads, and base stations.

(iv)Authorization: most effective legal nodes contain a selected interest.

(v)Integrity: ensures that no message or an entity may be changed because it negotiates from the sender to the receiver.

(vi)Freshness: it implies whether the records is recent and safeguards the network against replay assault.

(vii)Nonrepudiation: it protects from the malicious nodes that allows you to hide their activities.

closer to design of efficient safety solution, there are more demanding situations within the wireless sensor networks than wired networks. they're indexed as follows:

(i)wi-fi nature of communique,

(ii)useful resource inadequacy on sensor nodes,

(iii)very huge and dense sensor network,

(iv)unknown community topology,

(v)dynamic community topology.

Authentication in Wireless Sensor Networks

Authentication is a process by which the identity of a node in a network is verified and guarantees that the data or the control messages originate from an authenticated source. Various authentication procedures consist of(i)one-way authentication,(ii)two-way or mutual authentication,(iii)three-way authentication,(iv)implicit authentication.

1. One-Way Authentication

Only one message is transmitted from the sender node to the receiver node. This message will be able to create

(a)sender's identity,

(b)message that is generated by the sender,

(c)message that is intended to the receiver,

(d)message that is not altered during transit.

2. Two-Way or Mutual Authentication

Both entities can authenticate each other in a communication link. In WSN environments, this scheme not only means the authentication between normal nodes and the base station but also mentions the two counterparts that are secure of each other's identity.

3.Three-Way Authentication

A third message from the sender to the receiver is sent once the clocks of the nodes cannot be synchronized.

4.Implicit Authentication

Implicit authentication not only is accomplished as an independent process but also is the byproduct of other processes like key establishment. In WSNs, this type of authentication can minimize both operating complexity and energy consumption.

The authentication issues based on the node deployment are

(a) static deployment and

(b) dynamic deployment. In the former case, the nodes are static and are vulnerable to replay attacks. Authentication protocols should counteract these issues since the nodes are easily traceable. Some of the issues in the latter case are:

(a) moving node's reauthentication,

(b) node's movement that should be untraceable,

(c) message integrity,

(d) confidentiality, and

(e) node capture and compromise.

Various Authentication Protocols in Wireless Sensor Networks:

This section briefly discusses some of the popular authentication protocol schemes in wireless sensor networks.

1. Lightweight Dynamic User Authentication Scheme

WSN is deployed in a limited location that is separated into several zones. the usage of mobile gadgets, the legal users can access and communicate with the sensor nodes inside the WSN. This scheme includes three levels:(i)the registration section,(ii)the login phase,(iii)the authentication segment.

initially, a user ought to sign in with a call and a password at the sensor gateway node earlier than issuing any queries to the system. After a success registration, the user may also submit a query to the WSN device at any time inside a predefined length. relying upon the nature of the application, the predefined time period must be set in a distinctive way. The user desires to restart a new cycle by using doing the registration again, at the same time as the predefined time period has expired. A dynamic person authentication allows the real user to query the sensor information from someone of the sensor nodes. It imposes very less computational load, which can be evaluated the usage of simple strong-password based dynamic user authentication protocols for WSNs . This lightweight authentication scheme states that it's far comfy simplest against replay and forgery attacks.

An greater light-weight consumer authentication scheme [9] suggests that it is prone to replay and forgery attacks and additionally maintains the advantage of [5]. It now not best upholds all of the benefits but additionally improves its safety via enduring the weak point of the safety. The system is split into 4 levels: registration, login, authentication, and password-changing. Herein, the registration and password-changing stages are carried out via a comfy channel. It possesses numerous blessings, comprising resistance to each replay and forgery assaults, decreasing the hazard of consumer's password leakage, improved efficiency, and ability of changeable password [10].

2. Lightweight Trust Model

if you want to eat less reminiscence and energy, the light-weight schemes are brought [11–13]. In collaborative lightweight accept as true with-primarily based routing protocol (CLT), the memory consumption is decreased with the aid of the subsequent three steps:(i)first of all, the accept as true with is computed as superb integer inside the range from 0 to a hundred. It computes simplest one byte of reminiscence.(ii)This scheme does not directly store the computed price of agree with in the transaction table.(iii)The memory consumption is decreased drastically because the accept as true with level consumes handiest 3 bits of reminiscence.

This scheme additionally complements the packet transport ratio the usage of a trust management gadget. It notably decreases the power intake through averting promiscuous operation mode.

Conclusion:

protection is the essential challenge for the strength-confined WSN because of the wide security programs. In latest years, security has attracted quite a few attention and it's far very challenging to layout sturdy safety protocols. numerous schemes proposed on authentication are analyzed to perform confidentiality and authenticity of nodes. maximum authentication mechanisms recognition simplest on security, even as others offer proper scalability, minimized communication, and computation overhead. The authentication is an efficient technique to repel diverse assaults because it requires sharing of keys. it's miles therefore evident from the literature that an authentication scheme can lessen the computation value and store electricity. based on our comparisons and take a look at, we finish that authentication mechanism has been extensively used these days but still suffers from the subsequent troubles inclusive of complicated management of public key infrastructure and computational bottleneck which need to be resolved through destiny studies

References:

1. *X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, "An effective key management scheme for heterogeneous sensor networks," Ad Hoc Networks, vol. 5, no. 1, pp. 24–34, 2007.*
2. *D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," ACM Transactions on Information and System Security, vol. 8, no. 1, pp. 41–77, 2005.*
3. *M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic key management in sensor networks," IEEE Communications Magazine, vol. 44, no. 4, pp. 122–130, 2006.*
4. *J. Sen, "A survey on wireless sensor network security," International Journal of Communication Networks and Information Security, vol. 1, pp. 55–78, 2009*
5. *K. H. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, vol. 1, p. 8, IEEE, Taichung, Taiwan, June 2006.*
6. *T.-H. Lee, "Simple dynamic user authentication protocols for wireless sensor networks," in 2008 Second International Conference on Sensor Technologies and Applications (SENSORCOMM '08), pp. 657–660, Cap Esterel, France, August 2008.*
7. *B. Vaidya, J. Sá Silva, and J. J. P. C. Rodrigues, "Robust dynamic user authentication scheme for wireless sensor networks," in Proceedings of the 5th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet '09), pp. 88–91, ACM, October 2009.*
8. *O. Cheikhrouhou, A. Koubâa, M. Boujelben, and M. Abid, "A lightweight user authentication scheme for wireless sensor networks," in Proceedings of the ACS/IEEE International Conference on Computer Systems and Applications (AICCSA '10), pp. 1–7, Hammamet, Tunisia, May 2010.*
9. *H.-R. Tseng, R.-H. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in Proceedings of the 50th Annual IEEE Global Telecommunications Conference (GLOBECOM '07), pp. 986–990, Washington, DC, USA, November 2007.*
10. *A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor*

networks," Journal of Network and Computer Applications, vol. 35, no. 5, pp. 1646–1656, 2012

11. X. Anita, M. A. Bhagyaveni, and J. M. L. Manickam, "Collaborative lightweight trust management scheme for wireless sensor networks," Wireless Personal Communications, vol. 80, no. 1, pp. 117–140, 2015.
12. X. Fan and G. Gong, "Lpkm: a lightweight polynomial-based key management protocol for distributed wireless sensor networks," in Ad Hoc Networks, vol. 111 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 180–195, Springer, Berlin, Germany, 2013
13. M. Singh, A. R. Sardar, R. R. Sahoo, K. Majumder, S. Ray, and S. K. Sarkar, "Lightweight trust model for clustered WSN," in Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, pp. 765–773, Springer, 2015.
14. A. Fúster-Sabater, and J. M. Sierra, "A light-weight authentication scheme for wireless sensor networks," Ad Hoc Networks, vol. 9, no. 5, pp. 727–735, 2011.
15. S. Raja Rajeswari and V. Seenivasagam, "Secured energy conserving slot-based topology maintenance protocol for wireless sensor networks," Wireless Personal Communications, pp. 1–24, 2015.