ISSN: 2455 - 5630
International Journal of Scientific Research and Modern Education
Impact Factor 7.137, Special Issue, March 2020 – Conference Proceedings
International Conference on Rise of Disembedded Unilateral Economy: InnoVision in the Era of Deglobalization (KRUPACON 2019) On 8th & 9th November 2019 Organized By
Krupanidhi Group of Institutions, Bangalore, Karnataka

A SURVEY ON SECURITY PROTOCOLS IN WSN

Vijayamala S Yakri
Krupanidhi Group of Institutions, Bangalore, Karnataka

Cite This Article: Vijayamala S Yakri, "A Survey on Security Protocols in WSN", International Journal of Scientific Research and Modern Education, Special Issue, March, Page Number 1-2, 2020.

Abstract:
Wireless Sensor Network (WSN) is apromising technology currently and in the near future. Networks like Vehicular ad-hoc Network (VANET) and Internet of Things (IoT) are also emerging fast where WSN is used directly or indirectly. Over the course oftime the range of the network of wireless sensors expands so that protection for the node is important. We survey a wide range of available network security protocols that serve the WSN.

Key Words: VANET, IoT, WSN, Security Protocols, Etc.

Introduction:

The WSN is a series of different sensors in an environment that detects, computes and interacts with sensor nodes adjacent to it. The sensor nodes consume low power and have low memory. These sensor networks have a broad variety of applications from environmental sensing, management functions, industrial monitoring, machinery control, health monitoring, etc. The autonomous node array processes the information generated by the centralized node called sink and communicates it to the central node. The sink's location is mostly close to the sensor area. The data from the sensors can be processed locally in the sink node, or is routed to the centralized device through a gateway. These intermediate nodes called gateways are linked to the sensor nodes, Smartphone's, the Internet and so on.

Wireless Sensor Network Architecture:

The sensors in a WSN Architecture include the following components:

- A Transceiver
- Microcontroller
- Power Source
- Memory

The transceiver comprises of the transmitter and the receiver componentsto relay and receive radio signals using antennas. The microcontroller acts as the main brain which controls the major functions of the system like providing an interface between the transceiver circuit, memory and the power source, etc. Memory is the part where the data is stored and accessed whenever necessary.

Network Component of WSN:

Sensors/actuators relay/intermediate nodes, gateways and the application are the network portion of the wireless sensor network. In a simple WSN the data is collected from the application by the sensors/actuators and is relayed to the sensor node through a gateway. If the gap between the leaf nodes in the sensing area is high and the application is high an intermediate node or relay is used. The gateway acts as an intermediary between application and sensor for protocol transformation in this network component. The relay node acts as the router and the Leaf node is the sensor area endpoint.

Limitation in WSN:

Minimum Resource: The sensors or field instruments have low resources, such as a smaller supply of electricity, reduced computing power, limited memory, etc.

- Working Environment: The sensors are usually unattended or deployed in an hostile environment hence the sensors cannot be quickly recharged or replaced and can also be prone to physical attacks and damages.
- Random Topology: The average topology of the sensors is too difficult to find since the sensors are not uniformly distributed.
- Security: Protecting sensors and data is difficult as the sensors work in a hostile area and contact occur wirelessly.
- Redundant Data: In most situations, the WSN sensors send the data to neighbors to enable the data to be redundant.

Security Protocols for Wireless Sensor Network:

A. SPINS:

The SPINS (Security Protocols in sensor networks) protocol proposed by Adrian Perrig et al [4] is a fit of two WSN protocols, namely SNEP and µTESLA. The SNEP emphasizes on anonymity, honesty and security while the µTESLA focuses on broadcast validation.

i. SNEP:

The SNEP (Secure Network Encryption Protocol) uses a standard controller, at the sender and at the recipient end for proper functioning. In SNEP you can use the block counter mode to transform the plain text to cipher text (CTR). This requires a message authentication report code for authentication and honesty (MAC). The sender determines and adds the initial message to the MAC. When the recipient opens the message, the MAC is calculated and correlated with the sent MAC, if the message fits, the message is otherwise declined.

ii. µTESLA:

Valid broadcasting needs a symmetric cryptographic system with a high measurement and overhead memory that makes it difficult for the WSN to use this mechanism. In µTESLA, the delayed symmetrical key disclosure is added. The base station validates a packet by using a hidden key to compute a MAC on the packet. Node where the packet is placed in a buffer before the

base station receives the key. The key to validate the packet is used when the node receives the key. The MAC key is a central feature of the public function F in the core chain.It computes the Key Kusing the formula as given below

$$K_i = F(K_{i+1})$$

B. TINYSEC:

The TINYSEC [6] is a security protocol for the connection layer that offers all SNEP services. TINYSEC which does not use the counter for a cryptographic operation isthe key discrepancy between SNEP and TINYSEC. Tinysec comprises two flavors, namely Tinysec-AE and Tinysec-Auth. Both authentication and encryption are supported by TINYSEC-AE. Authentication is possible only in the TINYSEC-Auth. For authentication and encryption it uses cyber-block chaining.

C. MiniSec:

The MiniSec [5] is a low-power network layer protocol. In order to supply encodes to packets, it utilizes offset code book (OCB) modes. MiniSec has 2 modes: MiniSec-U and MiniSec-B. The unicast mode is here MiniSec-U and the broadcast mode is MiniSec-B. The way they use the counter in their operations varies between MiniSec-U and MiniSec-B.

D. LEAP:

The LEAP is a primary WSN executive protocol (Localized Encryption and Authentication Protocol). The Jump is intended to deliver secrecy and authentication.

Conclusion:

In this paper several WSN protection guidelines have been reviewed. The Wireless Sensor Network offers different degrees of protection. The use of the Wireless Sensor Network can be expanded from agriculture to military and health to industry by establishinglatest security protocols for the WSN.

Acknowledgement:

The authors express gratitude towards the assistance provided by The Management, Krupanidhi Group of Institutions (KGI) and Krupanidhi Research Incubation Centre, KGI in completing the research. I thank our Research Mentor who guided throughout the research and helped me in achieving the desired results.

References:

1. B. Ayyappan, P. Mohan Kumar, “Vehicular Ad Hoc Networks (VANET): Architecture, methodologies and design issues”, IEEE Conf Publication, Pages: 177 -180, 2016.
2. Priyanka, P, Ayyappan, B, “Wireless sensor networks -technologies, protocols, applications and simulators: A survey” JCPS Journal, 2015.
3. Monika Bhalla, Brijesh Kumar, Nitin Pandey, “SecurityProtocols for Wireless Sensor Networks”, 2015, ICGC loT - International Conf on Green Computing and Internet of Things, 978-1-4673-7910-6/15, IEEE, 2015.
4. Adrian Perrig, Robert Szewczyk, David Culler and J. D. Tygar, “SPINS: Security protocols for sensor networks”, In 7th Annual ACM International Conf on Mobile Computing and Networks-Mobi Com 2001, July 2001.
5. M. Luk, G. Mezzour, V. G. Ligor and A. Perrigo, “Mini Sec: A Secure Sensor Network Communication Architecture”, in IEEE International conf on Information Processing in Sensor Networks Cambridge, Massachusetts, USA, 2007
6. C. Karlof, D. Wagner, N. Sastry, “Tiny Sec: a link layersecurity architecture for wireless sensor networks”, in Second International conference on embedded networked sensor systems, Baltimore, MD, USA, pp162-175, 2004.
7. Fadi Aloul, Mokhtar Aboelaze, “Current and FutureTrends in Sensor Networks: A Survey”, IEEE-2005
8. Feng Rui, Hu Xiangdong, “Message Broadcast Authentication in μTESLA Based on Double Filtering Mechanism,” International Conference on Internet Technology and Applications (iT AP), Aug. 2011 pp.1, 4, 16-18