ISSN: 2321-7782 (Online)
Volume 2, Issue 3, March 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Review on Security and Privacy in Wireless Sensor Network

Shailesh N. Sisat[1]
Dept. of Electronics & Telecommunication
G. H. Raisoni C. O. E. & M., Amravati
Maharashtra – India

Shrikant J. Honade[2]
Assistant Professor
Dept. of Electronics & Telecommunication
G. H. Raisoni C. O. E. & M., Amravati
Maharashtra – India

Abstract: ***A wireless sensor network is mostly used to monitor environmental and physical conditions. It includes temperature, sound, pressure etc. and used to link data through the network to a main location. Wireless sensor network plays an important role in the military as well as commercial applications. The main objective of this paper is the review of various security threads and requirements in the wireless sensor network.***

Keywords: Wireless Sensor, Security, Privacy, WSN.

I. INTRODUCTION

Wireless sensor networks are very popular because of the reliable communication way solutions to military and commercial challenges. The low cost feature is the main advantage of wireless sensor network applications. But sensor networks also introduce severe resource constraints due to their lack of data storage and power. A key requirement under these circumstances is the secure and private broadcast of the message using wireless sensor network (WSN). The paper states the brief review of the importance of the security and privacy in the wireless sensor network. In section 2 we discuss the WSN security obstacles. Section 3 discusses the various security requirements. Section 4 discusses the attacks and various available solutions and section 5 discuss the Literature Survey on Security in Wireless Sensor Network.

Basic Wireless sensor Network Technology: WSNs form a particular class of ad hoc networks that operate with little or no infrastructure. WSNs are gaining momentum as they have great potential for both research and commercial applications. The sensor network nodes themselves are ideally low-priced, very small devices. They typically consist of a collection of application specific sensors, a wireless transceiver, a simple general purpose processor, possibly assisted by limited amount of special-purpose hardware, and an energy unit that may be a battery or a mechanism to obtain energy from the environment. We cannot assume that sensor nodes will be tam per resistant, although we will consider the availability of such tamper-resistant nodes for future applications. Sensor nodes are distributed over a potentially vast geographical area to form a static, multi-hop, self-organizing network. However, also mobile WSNs and mobility within WSN are conceivable [2]. Fig. 1 shows the basic wireless sensor node components.

II. OBSTACLES OF SENSOR SECURITY

The Obstacles in WSN security mechanism mainly divided in the following area.

- ***Limited Memory and Storage Space:*** A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm.

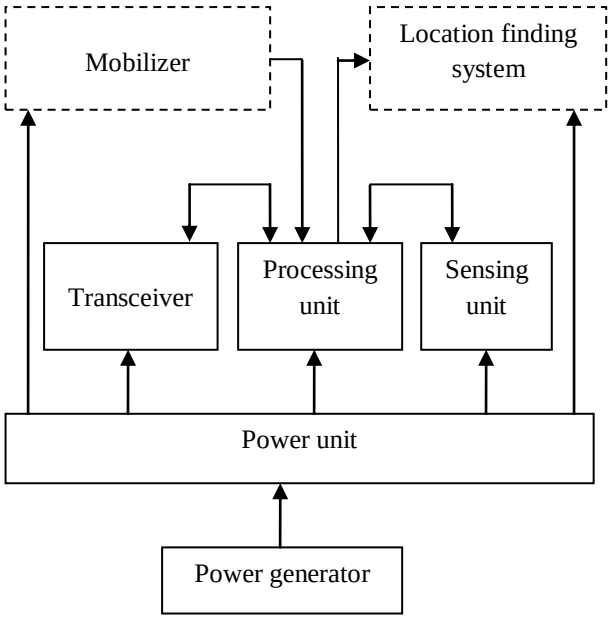

Fig. 1: Sensor Node component

For example, one common sensor type (TelosB) has a 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage [3]. With such a limitation, the software built for the sensor must also be quite small. The total code space of Tiny OS, the de-facto standard operating system for wireless sensors, is approximately 4K [3] [4], and the core scheduler occupies only 178 bytes. Therefore, the code size for the all security related code must also be small.

- ***Power Limitation:*** power limitation is most important constraint to wireless sensor network capabilities. When sensor nodes are attached in the field of wireless sensor network, the replacement or recharging may result in high cost. It implies in the proper selection of the battery that will extend the individual sensor node life present in the entire network. The power consumption must be considered while implementing a security protocol (eg. Cryptographic function) in the field of WSN.

III. SECURITY REQUIREMENT IN TYPICAL WSN

As discussed earlier the WSN is a delicate network in the specific area, following are the security requirements suited to the wireless sensor network.

- ***Authenticity and integrity:*** Malicious massage may change the originality of the data passing through the wireless sensor network, authentication of data as well as sender are also crucial security requirements. Source authentication provides the truthfulness of originality of the sender. Where, data authentication ensures the receiver that the data has not been modified during the transmission [5].

- ***Data Confidentiality:*** Main requirement of military and other commercial applications in the area of WSN is the data confidentiality. Data encryption is the standard method that avoids unwanted user interference in the wireless sensor network resulting to the data confidentiality.

- ***Availability:*** Sensor node must be available when needed. As sensor nodes have limited battery power, unnecessary computations may exhaust them before their normal lifetime and make them unavailable [5]. While implementing the security policies the unnecessary computations and hence the battery power must be taken into consideration.

- ***Freshness:*** When we accomplish the confidentiality and integrity, we must focus on the data freshness passing through the wireless sensor network. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed [3]. This requirement is especially important when there are shared-key strategies employed in the design.

Typically shared keys need to be changed over time. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack [3].

IV. ATTACKS IN WSN

Most network layer attacks against sensor networks fall into one of the following categories [6]

- Spoofed, altered, or replayed routing information
- Selective forwarding
- Sinkhole attacks
- Sybil attacks
- Wormholes
- HELLO flood attacks
- Acknowledgement spoofing

WSNs may affect due to the various types of attacks that are mainly categorized as,

- **Attacks on secrecy and authentication:** Standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets [5].
- **Attacks on network availability:** Attacks on availability are often referred to as denial-of-service (DoS) attacks. DoS attacks may target any layer of a sensor network [5].
- ***WSN Physical Attack:*** In this type of attack, attackers gain full control over some sensor nodes through direct physical access [7]. As attacker gets full control over sensor node in the WSN, it is very easy to get access over the node memory and gives opportunity to access the encrypted key stored on the node which restricts the unauthorized access to the network. In addition to the physical attack WSN affects due to other types of attacks that may categorized in different layers of the wireless sensor network.

1. ***WSN Physical layer attack:*** Physical layer is responsible for actual data transmission and reception, frequency selection, carrier frequency generation, signaling function and data encryption [8]. Data transmission, reception between various nodes of the WSN results into the radio interference and jamming.

- ***Jamming:*** Jamming is one of the most common attack done by adversaries by knowing the transmission frequencies used in the wireless sensor network.

2. ***WSN Link Layer attack:*** The data link layer is responsible for the multiplexing of data streams, data frame detection, medium access and error control. This layer is vulnerable to data collision when more than one sender tries to send data on a single transmission channel [5].

- ***DoS Attack by Collision Generation:*** In link year, collision is generated to exhaust the sensor node's energy. In order to generate collision, the attacker listens to the transmissions in WSN. When he finds out the starting of a message, he sends his own radio signal for a small amount of time to interfere with the message [7] [5] which cause CRC error at the receiving end. Because of this attack, the receivers cannot receive the message correctly [5].

3. ***WSN Network Layer attack:*** Messages routing from one to another node is the responsibility of network layer. The network layer for WSN is usually designed considering the power efficiency and data centric characteristics of WSN [5]. Following are some selected attacks that interferes the network layer of WSN.

- ***Selective forwarding:*** Selective forwarding is an attack where compromised or malicious node just drops packets of its interest and selectively forwards packets to minimize the suspicion to the neighbour nodes. The impact becomes worse when these malicious nodes are at closer to the base station [9] [5]. Then many sensor nodes route messages through these malicious nodes. As a consequence of this attack, a WSN may give wrong observation about the environment which affects badly the purpose of mission critical applications such as, military surveillance and forest fire monitoring [5].

- ***Sinkhole attack:*** In sinkhole attack, a compromised node attracts a large number of traffic of surrounding neighbours by spoofing or replaying an advertisement of high quality route to the base station [5]. Also known as black holes attack. Black hole attack affects on various parameters of WSN like energy, delay etc.

- ***Wormhole Attack:*** Wormhole is a critical attack, where the attacker receives packets at one point in the network, tunnels them through a less latency link than the network links to another point in the network and replay packets there locally [10] [5]. This convinces the neighbour nodes of these two end points that these two distant points at either end of the tunnel are very close to each other. If one end point of the tunnel is at near to the base station, the wormhole tunnel can attract significant amount of data traffic to disrupt the routing and operational functionality of WSN. In this case, the attack is similar to sinkhole as the adversary at the other side of the tunnel advertises a better route to the base station [5].

- ***Sybil Attack:*** In Sybil attack, a malicious or subverted node forges the identities of more than one node or fabricates identity. This attack has significant effect in geographic routing protocols [5]. The fake node implies various identities to other nodes in the network and thus occurs to be in more than one place at a time. In this way, it disturbs the geographical routing protocols. It can collide the routing algorithms by constructing many routes from only one node [11].

4. WSN Transport Layer attack: In network layer end to end connections are managed.

- ***WSN Flooding Attack:*** According to [12] and [13] [5], at this layer, adversaries exploit the protocols that maintain state at either end of the connection. For example, adversary sends many connection establishment requests to the victim node to exhaust its resources causing the Flooding attack. One solution against this attack is to limit the number of connections that a node can make. But, this can prevent legitimate nodes to connect to the victim node [5].

V. Literature Survey on Security in Wireless Sensor Network

However realization of sensor networks needs to satisfy the constraints introduced by factors such as cost, fault tolerance and power consumption. Since these constraints are highly stringent and specific for sensor network, new wireless techniques are required [1].

Dirk WESTHOFF [2] have focused on Nodes that compose a WSN are typically small and have very limited communication, computation, storage and power capabilities. The Berkeley Motes use an 8-bit 4MHz Micro-controller (MCU) with 4KB of memory and a radio transceiver with a maximum of 10kbps data rate. To keep costs low, most sensors are not tamper-resistant, which impacts security. Limited computing and storage capabilities make modular arithmetic with large numbers difficult and thus asymmetric (public key) cryptography unsuitable [2].

There is no standard security mechanism that can provide overall security for WSN. Providing such mechanism is not possible also as WSNs are implemented in various application domains with different level of security requirements. Designing a secure WSN needs proper mapping of security solutions or mechanisms with different security aspects. This also imposes a research challenge for WSN security. As wireless sensor networks continue to grow and become more common, we expect that further expectations of security will be required of these wireless sensor network applications. In particular, the addition of public key cryptography and the addition of public-key based key management [5].

RC5 is cryptographic algorithm, for which many parameters such as key size, block size and number of rounds can be adjusted to tradeoff security strength with power consumption and computational overhead [14].

RC6, which is a simple, fast, and secure block cipher, was the final candidate algorithm in the AES project of the United States and the NESSIE project of Europe. It requires 128 bit and variable-length block cipher encryption algorithm. RC6 has a modified Feistel structure [15].

Like RC5, RC6 is a fully parameterized family of encryption algorithms. A version of RC6 is more accurately specified as RC6-w/r/b where the word size is w bits, encryption consists of a nonnegative number of rounds r and b denotes the length of the encryption key in bytes. Since the AES submission is targeted at w = 32 and r = 20, we shall use RC6 as shorthand to refer to such versions [16].

The sensor network is one new research area of computer science technology and has the widespread application prospect. This project includes use of ZigBee technology. ZigBee technology is not brand-new standard completely. Its PHY level, MAC level and link level have used IEEE 802.15.4 protocol standard, but has carried on consummation and expansion. Its network level and high level application standard has been established by the ZigBee alliance [17].

Proposal for a public key cryptography based protocol for user Authentication and Session key establishment between external agent and a sensor in a secure manner [18].

It is possible for an optimized C implantation of AES encryption –decryption to match the communication speed of a Zigbee radio. It is observed that computational speed increases with reducing memory footprints. In future work it is possible to use developed encryption-decryption scheme as a primitive in a secure application and to developed efficient interface with other primitives such as authentication [19].

VI. WSN SECURITY SOLUTIONS

Cryptography and secure routing protocols provides the defense against the security in WSN.

VII. CONCLUSION AND FUTURE WORK

This paper gives an idea about the basic wireless sensor network and its major security issues and basic requirements. However WSNs are used for secrete communications e.g. military applications, focus should be on data security while designing the WSN. The future work for this research area will include the implementation of RC6 Algorithm in WSN and comparative study of various parameters with the RC5 Algorithm.

Acknowledgement

The author sincerely thanks to Prof. Shrikant J. Honade, Assistant Professor, G.H.R.C.E.M., Amravati, Dr. P. V. Ingole, Principal, G.H.R.C.E.M Amravati and Prof. N. N. Mandaogade, Head of E & TC Department G.H.R.C.E.M Amravati for their valuable suggestion, criticism and time to time encouragement.

References

1. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. “A survey on sensor networks”, IEEE Communications Magazine, 40(8):102–114, August 2002.
2. Dirk WESTHOFF, Joao GIRAO, Amardeo SARMA, “Security Solutions for Wireless Sensor Networks”, Nec Technical Journal vol.1 no.3/2006.
3. Security in Distributed, Grid, and Pervasive Computing Yang Xiao,(Eds.) pp. C 2006 Auerbach Publications, CRC Press.
4. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. E. Culler, and K. Pister. “System architecture directions for networked sensors”, Architectural Support for Programming Languages and Operating Systems, 2000.
5. Deepika Thakral, Neha Dureja “A Review on Security Issues in Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012
6. Karlof, C.; Wagner, D., "Secure routing in wireless sensor networks: attacks and countermeasures," Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on , vol., no., pp.113,127, 11 May 2003
7. Z. Tanveer and Z. Albert. “Security issues in wireless sensor networks”, In ICSNC ’06: Proceedings of the International Conference on Systems and Networks Communication, page 40, Washington, DC, USA, 2006. IEEE Computer Society.

8. John PaulWalters, Zhengqiang Liang,Weisong Shi and Vipin Chaudhary. "Wireless sensor network security: A survey" Security in Distributed, Grid, and Pervasive Computing", 2006.
9. Mayank Saraogi. "Security in Wireless Sensor Networks", ACM SenSys, 2004.
10. I. Khalil, S. Bagchi, N. B. Shroff. Liteworp, "Detection and isolation of the wormhole attack in static multihop wireless networks", Comput. Netw., 51(13):3750– 3772, 2007.
11. Ashima single, Ratika Sachdeva, "Review on Security Issues and Attacks in Wireless Sensor Network", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 4, April 2013
12. A. Wood and J. Stankovic. "Denial of service in sensor networks", Computer, vol 35, page 54U˝62, 2002.
13. D. R. Raymond and S. F. Midkiff. "Denial-of service in wireless sensor networks: Attacks and Defenses", IEEE Pervasive Computing, volume 7, 2008.
14. Dr Radhika K R, "A Novel Symmetric Key Encryption Algorithm Based On RC5 in Wireless Sensor Network", International Journal of Emerging Technology and Advance Engineering, Volume 3, Issue 6, June 2013
15. Gil-Ho Kim, Jong-Nam Kim, Gyeong-Yeon Cho, Dept of Computer Engineering PuKyong National Univ. "An improved RC6 algorithm with the same structure of encryption and decryption", Advanced Communication Technology, ICACT 2009. 11th International Conference (Volume: 02).
16. Harsh Kumar Verma, Ravindra Kumar Singh, "Enhancement of RC6 Block Cipher Algorithm and Comparison with RC5 & RC6", 978-1-4673-4529-3/12/$31.00c_2012 IEEE.
17. Changjiang Li, Yufen Wang, "The Application Research of Wireless Sensor Network Based on ZigBee", 2010 Second International Conference on MultiMedia and Information Technology, 43978-0-7695-4008-5/10 $26.00 © 2010 IEEE DOI 10.1109/MMIT.2010.143.
18. Vorugunti Chandra Sekhar, Mrudula Sarvabhatla, "Security In Wireless Sensor Networks With Public Key Techniques", International Conference on Computer Communication and Informatics (ICCCI), Jan. 10 – 12, 2012, Coimbatore, INDIA
19. Shammi Didla, Aaron Ault,"Optimizing AES for Embendded Devices and Wireless Sensor Networks", ICST, Belgium ©2008 ISBN: 978-963-9799-24-0

AUTHOR(S) PROFILE

Shailesh N. Sisat received the B.E. Degree in Electronics & Telecommunication Engineering from P.R.M.I.T.&R. Badnera Rly., S.G.B. Amravati University, Maharashtra, India. Presently he is second year M.E. student in department of Electronics and Telecommunication, G.H.Raisoni college of Engineering and Management, Amravati, Maharashtra, India.

Prof. Shrikant J. Honade received the B. E. degree in Electronics and Telecommunication from H. V. P. M's College of Engineering, Amravati and M. Tech degree in Electronic Systems and Communication from Govt. College of Engineering, Amravati, Maharashtra, India. Presently he is working as Assistant Professor in the Department of Electronics & Telecommunication Engineering, G.H.Raisoni C.O.E. & M. Amravati, Maharashtra, India.

