International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Providing Security for Wireless Sensor Networks Using Secure Protocol

Tabbasum Sajjan Magdum[1], Y. B. Gurav[2]

[1]Department of Computer Engineering, P.V.P.I.T. Bavdhan, Pune, Maharashtra, India

[2]Professor, Department of Computer Engineering, P.V.P.I.T. Bavdhan, Pune, Maharashtra, India

Abstract: ***In wireless sensor networks, it is necessary to restrict the system access, while messages from unknowns won't be sent in the networks. The WSNs uses data-centric multi-hop correspondence that thusly, demands the security support to be created at the link layer instead of being at the application layer, as when all is said in completed networks. Our aim is to explore security threats and challenges in sensor network. Secure protocol is a productive wireless sensor protocol which provides validation by means of CFA, avoids unapproved access to data using MDACP. In this paper, we present the design, usage, and assessment of a secure system access system for wireless sensor networks. The sensor node's constrained storage, the storage condition of these protocols is undesirable. The proposed system includes the channel based methodology to evacuate replay packets and to minimize storage overhead in replay location. The proposed methodology consumes a great deal fewer storage and vitality than several methods.***

Keywords: Wireless Sensor Network; MDACP; CFA; multi-hop.

1. Introduction

Wireless sensor network is research engineering method because of vast variation of applications that applies to virtual world. Recent innovative enhancements have made the sending of small, low-cost, low-power distributed devices, which are prepared for nearby pro-cessing and wireless communication. Every node contains processing capability[6]. It might be contain numerous types of memory (project, data and memories), RF transceiver, power sources (e.g., batteries and solar cells), and assist several sensors and actuators. WSN has basic applications like military applications and examine patient in hospitals. The organization of these networks in military applications with minimal power and memory, model the framework of a security protocol extremely difficult. It is necessary to design appropriate security mechanism to manage sensor network constraints[3]. In wireless sensor networks[10], it is discriminating to restrict the network access just too trained sensor *nodes*, while messages from unknowns should not be sent in the networks.

Since sensor nodes are extremely constrained in terms of resources, satisfying the security protocols in an effective way using less energy, computational time and memory space. The noticeable solution to anticipating security issues because of eavesdropping is to encrypt all movement passing through the network. Network nodes are often sent through an unreliable scattering process, such as an air drop [1]. Loading each node with a set of pair wise keys for each node in the network is illogical because the memory of a node is usually too small to save thousands of keys. WSN are described by severe constraints in power, computational resources, memory, and bandwidth and have lesser physical size with low power consumption [2][3]. Confirming security in WSNs requires adjusting the conventional security protocols to the resource constrained WSN environments, with slight overhead.

Protocols in WSN

For secure network protocol, a huge portion of skills has been generated including Zigbee, SPIN, TINYSEC, Minisec. Sensor protocol for information by means of negotiation: It involves of two building square: SNEP and TESLA. SNEP (secure network encryption protocol) have several advantages. First one is, low communication overhead because it improves just eight-bytes each message. Second one, it can't convey the counter values by keeping state at both source and destination. Third one is, Data privacy can be skillful using encryption, yet just encryption is not enough. Fourth one is, semantic security can be skilled using randomization strategy. At last two collecting data verification and data uprightness can be accomplished by message authentication code. Second section is TESLA(timed efficient stream loss tolerant authentication) which provides verification for the initial packets using the idea of digital signature which is exclusive for sensor nodes.

Minor Security Protocol

TINYSEC is initially well-known link layer protocol to achieve low memory usage. Several sensors can deliver on network by using multi-hop topology to base station. Every node on network directs a packet to the base station in response; energy and bandwidth are lost. To kill these undesirable messages, to decrease activity and save energy, sensor networks exploits in-network processing that contains aggregation and copy elimination.

Minisec protocol

Minisec is a network layer protocol which merges both: low energy consumption and high security. Authentication can be achieved to using square figure mode of operation. It offers replay protection which is not in Tiny Sec. Mini Sec uses two techniques OCB Encryption and channel based methodology for low energy consumption [4].

Zigbee Protocol
Zigbee provides a higher amount of security than Tinyec since it is not controlled to using a far reaching key. By keeping an every message counter as the Initialization Vector (IV), Zigbee protects against message replay attacks. First, Zigbee sends the complete 8-byte with each one packet, ensuing in high communication overhead and high energy consumption by the radio. Also, Zigbee requires every sender state, which consumes a lot of memory as the quantity of participants increases [10].

2. Related Work

A. Authentication

Authentication is a procedure of ensuring of sensor nodes, cluster heads and base stations are confirmed before giving a constrained resource or uncovering information. K Han et al in [4], implemented an proficient model for confirmed key assertion in dynamic WSN and this protocol enables to moderate authentication process for portable node and can be used in several used of WSN. MP et al in [5], proposed a user authentication approach which is a variant of strong password based solution. Wong et al in [6], implemented an element user authentication approach for WSN.

Zhu et al in [7], implemented that every node creates a one way key chain and sends the dedication of it to their neighbors. The accepting node can check the validation of the key, based on the dedication it has officially acquired. This approach does not give a solution to inside attacks as the opponent knows nodes cluster key. Huang et al in [8], implemented a self-sorting out calculation using ECC which has phases
Phase1: Implicit Certificate Creation Process and
Phase 2: Hybrid key Formation Process.

Supports dynamic node re-authentication yet the inventor did not state it. Mahagoub in [9], implemented an effectual model is executed by using halfway key escrow table. By using this table the sink can self-produce a shared key for the attached nodes to support node flexibility. Dong et al in [10], overcomes the malicious node attack, by establishing a gathering key with the neighbors node and sifting out the misbehaving nodes. Ravi et al in [11], proposed a PKC certification based approach for user authentication, authentication being produced by the
Sink.

B. Access Control
The principle calculation measured for this sort of access control (authentication just) is a cryptographic test response protocol, in which a user and network are mutually verified to every other. In [11], the energy efficient access control approach is presented for WSNs based on Elliptic Curve Cryptography (ECC). The proposed approach has better execution contrasted with the other PKC based access control schemes and fair performance contrasted with Secret Key Cryptography (SKC) based ones. In [3], the author presented element user authentication strategy for WSNs. In this approach, the approved users can access any of the sensor nodes in WSNs using portable devices, such as PDAs, PCs, and so on.

C. Replay
Replay Protection:
Terminology
Syverson classified the replay attacks in two types i.e. the replay attack on the protocol run at the destination and that at the source. In [4], Paul Syverson gives an aspect taxonomy scientific categorization of replay attacks which specify what information can be used as the basis to distinguish replay attack. In [7], Li Gong presents a discussed on the decision of recognizing the freshness identifier, to be utilized with the message.

3. Implementation Details

A. System Overview
The following Figure 1. Shows the proposed system architecture.

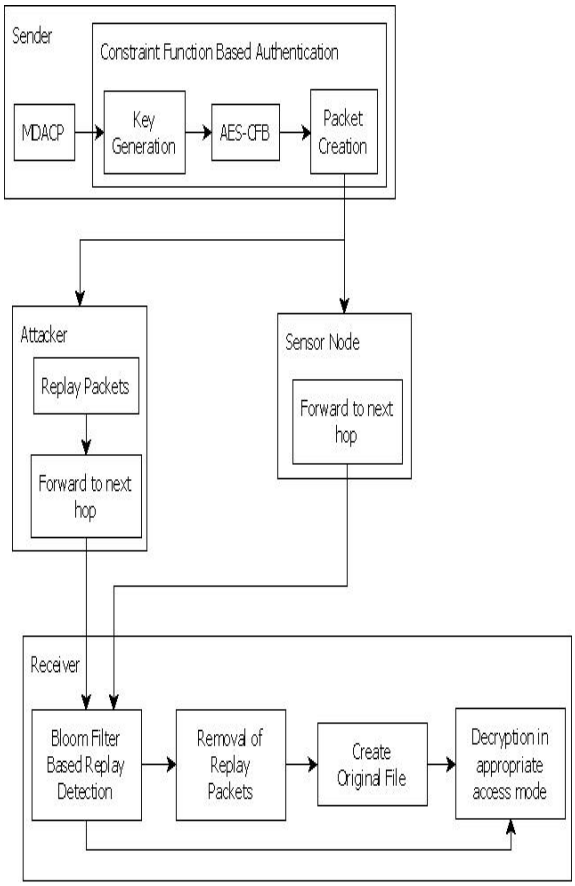

Figure 1: System Architecture

Data Authentication
This module includes the implementation of encryption and decryption algorithms by using Advanced Encryption Standard (Cipher feedback mode), which permits to transmit the data through air and constrained function based authentication is used to prevent an adversary from spoofing packets. For Data Authentication we are used AES encryption and decryption algorithm for authentication.

Replay Detection and jamming
In this Module we are applying replay detection algorithm for detecting Replay packets and our system works only for detecting replay packet and to filter the replay packet.

Data Access

This module provides permit oreny data access based upon a set of rules, which are frequently used to protect the data from unauthorized access while permitting legitimate communications to pass using Memory Data access control policy. In MDACP, every user is connected with a key (e.g., a prime number) and every file is associated with a lock value. Matrix contains different types of access modes for e.g. 0 indicate none as access mode, it means user not having any authority to access file. 1 indicate read as access mode. It means user having authority to read file. 2 indicates write as access mode. It means user having authority to read file. 3 indicate own as access mode. It means user having authority to read as well as write file.

B. Algorithm

Algorithm 1 For Replay Bloom Filter Attack
1: IFor(Each packet)
2: {
3: applyHash (packet)
4: {
5: For(i=0;I ¡4;i++)f
6: String Value =Apply SHA(packet);
7: }
8: }
9: If(Filter created)
10: {
11: If(String Value is present)
12: {
13: Replay Packet is detected .
14: }
15: Else {
16: Filter Add(packet);
17: }
18: If(replay packet detected)
19: }
20: Find real replay attacked by trace back scheme;

C. Mathematical Model

1.At Sender Timestamp (Ts) is calculated for each sending packet
T_s=$\sum_{i=1}^{N}(P_i)$
Where (P_i) are sending packet
Timestamp T_s - Time at which packet send .

2.Calculate Time stamp (T_r) for each receiving packet
T_d=$\sum_{i=1}^{N}(R_i)$
And (R_i) are the Receiving packet
Timestamp (T_r) - Time at which packets are received.
Threshold is calculate for Jamming detection.

3.Calculate Threshold T_{sd}:
$T_{sd} = \sum_{i=1}^{N} T_d - \sum_{i=1}^{N} T_s$
Where, T_d and T_s are the time stamps for all packets at receiver and sender respectively.

For each communication the Time for all the packet sending is calculated and this time is compared with the generated threshold .

Replay Detection

1. **For** For Incoming packets set at receiver P = {p1, p2, p3,.....,pn}.
   P is set packet may contain replay packet
2. Let Buffer B of size n.
   Buffer B[n];
3. D is the set of duplicate packet D= {d1,d2,d3.....dn}.
4. For each packet in set P.
   Generate hash for P;
   If (B[n] contain Duplicate Hash)
   Replay packet detected ;
   Filter Packet P
   Else Receive packet
   add packet in B[];
5. After Filtering R = {R1,R2,R3,....,Rn}.
6. R set Of original Packets.

D. Experimental Setup

The system is built using Java framework(version jdk 6)on Windows platform. The Netbeans (version 6.9) is used as a development tool. The system doesn't require any specific hardware to run, any standard machine is capable of running the application.

4. Results and Discussion

A. Result

The following Table I shows number of packets send without security and with security

Table 1: Number of Packets Sends Vs Time In Ms

Number of packets	Without security	With security
10	7345	4300
20	14415	7350
30	19462	9396
40	27516	11470
50	36560	13535
60	44610	15540

The following Figure 2 shows graph of number of packets send VS time in ms. The following graph shows that packets without security require more time for sending packets compared to with security.

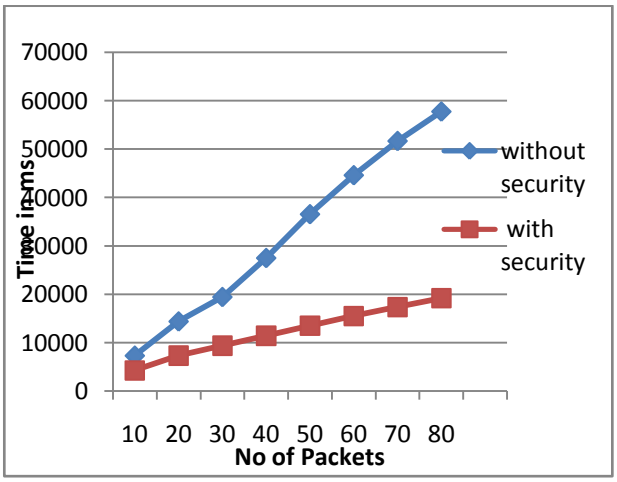

Figure 2: Graph for number of packets send VS times in ms.

5. Conclusion

Proposed system will detect Jamming and Replay attack by using minimum energy minimization and furthermore prevention by packet filtering technique. We are decreasing the memory usage for detection of replay attack by using hash procedure. By using hash function the energy usage is amplified and Performance is improved. Also the security is increased by using access control mechanism. Secure protocol is ready to achieve the goals of considerably less energy consumption and higher security than previous works. This helps to use the proposed implementation on any operating system. For Future work, we can find the actual source of attack from where the replay and jamming attack is happening.

6. Acknowledgment

We are thankful to the authorities of Savitribai Phule pune University, Pune for their constant guidelines . We also thankful to my guide & college authorities for providing constant guidelines and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

References

[1] Yao-Tung Tsou, Chun-Shien Lu, Member, IEEE, and Sy-Yen Kuo, Fellow, IEEE, "MoteSec-Aware: A Practical Secure Mechanism for- Wireless Sensor Networks" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 6, JUNE 2013.
[2] Dalit NaorMoniNaor Jeff Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers".
[3] Chia-Mu Yu, Chun-ShienLu,andSy-Yen Kuo,"A Constrained Function Based Message Authentication Scheme for Sensor Networks" IEEE Communications Society.
[4] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, 'MiniSec: a secure sensor network communication architecture,' in Proc. 2007 International Conference on Information Processing in Sensor Networks, pp. 479488.
[5] Chris Karlof, Naveen Sastry, David Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks".
[6] Kun Sun, An Liu, "Securing Network Access in Wireless Sensor Networks" the Department of Homeland Security under grant NBCHC080061.
[7] Madhumita Panda, "Security Threats at Each Layer of Wireless Sensor Networks" Volume 3, Issue 11, November 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.
[8] SAURABH GANERIWAL, "Secure Time Synchronization in Sensor Networks" ACM Transactions on Information and Systems Security, Vol.11, No. 4, Article 23, Pub. date: July 2008.
[9] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, "SPINS: Security Protocols for Sensor Networks" In Proceedings of the 7th Annual International Conference on Mobile Computing and Networks (MOBICOM), July 2001, pp. 189-199
[10] Jin Li, Xiaofeng Chen, Mingqiang Li, Jingwei Li, Patrick P.C. Lee, and Wenjing Lou, "Secure Deduplication with Efficient and Reliable Convergent Key Management" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 6, JUNE 2014.
[11] A. R. Uttarkar, H. A. Hingoliwala, "Secure System Practices and Data Access Management in Wireless Sensor Network" International Journal of Computer Applications (0975 8887) Volume 91 No.11, April 2014.
[12] DeveshJinwala*1, Dhiren Patel2 and Kankar Dasgupta, "FlexiSec: A Configurable Link Layer Security Architecture for Wireless Sensor Networks" Journal of Information Assurance and Security 4 (2009) 582- 603