IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Secure Protocol for Replay and Jamming Attack Detection in Wireless Sensor Network

Gaurav S. Deore[1], Chandrashekhar S. Khasnis[2], Mrs. U.H.Wanaskar[3]

Student, Computer Engineering, PVPIT, Pune, India[1, 2]

Assistant Professor, Computer Engineering, PVPIT, Pune, India [3]

Abstract: In wireless sensor networks, it is elementary to restrict the system access just to trained sensor nodes, while messages from unknowns won't be sent in the networks. In expansion, the WSNs uses data-centric multi-hop correspondence that thusly, demands the security support to be created at the link layer (increasing the cost of security related operations), instead of being at the application layer, as when all is said in completed networks. The aim of this paper is to explore the security threats and challenges in sensor networks. Motesec 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. Many protocols have been projected for replay attack assurance, however they involve higher storage limit. Because of the sensor node's constrained storage, the storage condition of these protocols is undesirable. By noticing this limitation, the existing protocols are used just for replay and jamming attack discovery. The proposed system includes the channel based methodology to evacuate replay packets and to minimize storage overhead in replay location. The result demonstrates that proposed methodology consumes a great deal fewer storage and vitality than several methods.

Keywords: Sensor networks, security, Bloom Filter, Replay Attack, Jamming Attack.

I. INTRODUCTION

Wireless Sensor Network is research engineering methodology because of their vast variation of applications that links open applications to virtual world. Recent innovative enhancements have made the sending of small, low-cost, low power distributed devices, which are prepared for nearby processing and wireless communication such kind of devices are indicated as sensor nodes. Every node composed of processing capability (CPU/DSP chips, microcontrollers) [6]. It might be containing numerous types of memory (project, data and memories), RF transceiver, power sources (e.g., batteries and solar cells), and assist several sensors and actuators. An extending usage of wireless sensor networks forever basic applications such as military applications and examine patient in hospitals. These applications create its critical to have a decent security organization for sensor networks. The organization of these networks in military applications with minimal power and memory, model the framework of a security protocol extremely difficult. WSNs are neglect to resist several dissimilar types of attack because of unprotected and risky nature of communication channel, sending in aggressor situation, broadcast approach of communication, limited the number of resources; consequently, security is needed necessity for these networks. 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. Additionally, unknowns can't eavesdrop, modify or forge packets from trained nodes inside the sensor network. 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) without sacrificing the strength of their security properties is one of the major challenges [6].

The noticeable solution to anticipating security issues because of eavesdropping is to encrypt all movement passing through the network. This involves the distribution of cryptographic keys for encryption of data. Automatic solutions for the distribution of keys don't work in WSN's. Network nodes are often sent through an unreliable scattering process, such as an air drop [1].

As such, we generally assume that the topography of the network can't be identified ahead of time. This means that we can't preload each node with the keys of its prompt neighbours. 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. Public key algorithms are generally considered to be too computationally severe for resource constrained WSN nodes [11].

II. LITERATURE SURVEY

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. Location information and key administration messages begin from the right source.

DOI 10.17148/IJARCCE.2016.55167

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. It permits the real users to question the sensor data from any of the sensor nodes by imposing fewer computational burdens. This approach stated that it is secure against replay and forgery attacks in which it fails.

Zhu et al in [7], implemented that every node creates an one-way key chain and sends the dedication of it to their neighbours. In the event that a node wants to send a message to its neighbours, it attaches the following authorization key from its key tie to the message. 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. Proposed approach has major issue where every sensor node must have immediate contact with the CA which would be a bottleneck.

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 neighbours 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. This scheme is powerless against DOS attack. Omar et al in, proposed a key distribution scheme for element conferences.

In this scheme a trusted server allocates private pieces of information to a set of users. Every part of any gathering of users of a given size can process a secure gathering key.

B. Access Control

Most of access control procedures presented so far for WSNs concentrates on the authentication step of the access control while overlooking the authorization step. 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). Authors proposed an energy efficient technique to use ECC (which is a Public Key Cryptography (PKC) scheme). 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. Then again, the proposed approach needs the Key Distribution Center to be accessible constantly, which may not be the situation, may cause users to be terminates by the access controlling nodes of the WSN.

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. The proposed scheme permits real users to question sensor data at any of the sensor nodes in an incorrect way. It executes next to no computational load and requires just simple operations.

C. Replay

Replay Protection:
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 aspect taxonomy scientific categorization of replay attacks which specify what information can be used as the basis to distinguish replay attack.

In [5] T.y.c. Charm and S.S. Lam describe the standard of full information, i.e. labelling all information accessible with the source, at the time of transmission of the message. In [6] Aura proposes labelling just a hash of piece of some information that is as of now known to the receiver.

In [7], Li Gong presents a discussed on the decision of recognizing the freshness identifier, to be utilized with the message.

III. MOTIVATION AND PROBLEM STATEMENT

Wireless Sensor Networks (WSN) is invading our everyday life with their proliferating applications which cover environmental observation, homeland security, building and factory monitoring and personal healthcare. The small dimensions of sensor nodes combined with their low cost, usability properties, motivates the researcher to work towards this area. The system implements for removing the drawbacks of existing system. The drawbacks are: Time consuming because of ECC, Password could be easily disposed, cannot protect against forgery, replay attack, Trouble while changing own password. Moreover, several real-world scenarios, including community/environment monitoring, smart

DOI 10.17148/IJARCCE.2016.55167

home, need data transmitted over the network and data stored in node's memories. Due to the resource-limited sensor nodes, traditional network security mechanisms are not suitable for WSNs. Inspired by the above challenges; we study the issues of secure network protocol and data access control in WSNs in order to avoid data leaking to the adversary or unauthorized party. In fact, we are aware that a secure mechanism suitable for wireless sensor networks has not been constructed yet, as the related works reviewed below indicate.

A. Problem Definition

Reducing storage overhead and detecting replay attack by filter based approach and detection of jamming attack by counter based approach in Wireless Sensor Networks.

B. Purpose

The purpose of this document is to describe the functioning of the protocol which is used to detect attacks and also provide a security mechanism like authentication, access control, integrity, and confidentiality. The detailed description of the proposed work is illustrated in the document. The work can be deployed on the Wireless Sensor Networks that are used in various applications. The existing MoteSec Aware protocol is improved by adding features like, attack detection technique and using a filter based approach for reducing the storage overhead while detecting the replay attack.

C. Scope of the Work

The scope of this work is is to explore the security threats and challenges in sensor networks. The proposed system includes the channel based methodology to evacuate replay packets and to minimize storage overhead in replay location. The result demonstrates that proposed methodology consumes a great deal fewer storage and vitality than several methods.

IV. PROPOSED SYSTEM

The security of communication and access control in Wireless Sensor Networks (WSNs) is of paramount importance. MoteSec-Aware is practical secure mechanism for wireless sensor networks which deals with Authentication using constrained function based authentication, for confidentiality, used advanced encryption standard in cipher feedback mode. On the other hand, Memory Data Access Control Policy (MDACP) is presented to achieve the goal of data access control, filter based approach is used for detecting replay attack and exible deterministic packet marking approach for detecting attack for securing the protocol.

A. Objectives

The main goal and objective of the project is to detect replay attack by using bloom filter based approach to reduce storage overhead and making it energy efficient and dropping replayed packet and to also detect jamming attack by counter based approach. It aim to provide Security primitives like Authentication, Confidentiality, Integrity, Access rights to authorized user..

V. SYSTEM ARCHITECTURE

The following system architecture shows Receiver node sends request to sender node for data. A sender node accepts the request of receiver node and read the value from MDACP matrix and encrypts requested data. And send data to the intermediate node. At sender node after receiving encrypted data it replay detection if attack found it drop the replay packets and if it is not found then it create original file and decrypt data.

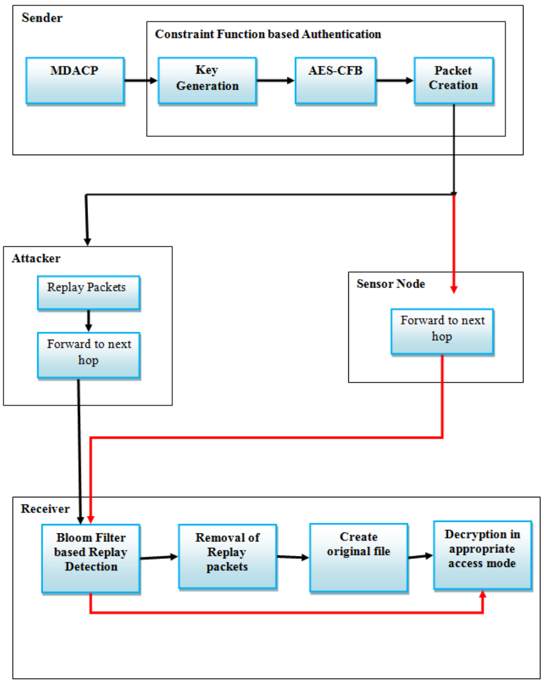


Fig 1: System Architecture

Ensuring the security of communication and access control in Wireless Sensor Networks WSNs) is of paramount importance. MoteSec-Aware is practical secure mechanism for wireless sensor networks which deals with Authentication using constrained function based authentication, For confidentiality, used advanced encryption standard in cipher feedback mode. On the other hand, Memory Data Access Control Policy (MDACP) is presented to achieve the goal of data access control, filter based approach is used for detecting replay attack and exible deterministic packet marking approach for detecting attack for securing the protocol. The results demonstrate that MoteSec-Aware consumes much less energy, yet achieves higher security than several state-of-the-art methods.

The system implements for removing the drawbacks of existing system. The drawbacks are: Time consuming because of ECC, Password could be easily disposed, Cannot protect against forgery, replay attack, Trouble while changing own password. Moreover, several real-world scenarios, including community/environment monitoring, smart home, need data transmitted over the network and data stored in node's memories. Due to the resource-limited sensor nodes, traditional network security mechanisms are not suitable for WSNs.

VI. ALGORITHM

Algorithm: For Replay Bloom Filter Attack

```
I For ( Each packet)
{
    Apply Hash (packet)
    {
        For (i=0; I! 4;i++)f
            String Value =Apply SHA (packet);
    }
}
If (Filter created)
{
    If (String Value is present)
    {
        Replay Packet is detected.
    }
    Else f
        Filter Add (packet);
}
If (replay packet detected)
{
    Find real replay attacked by traceback scheme;
}
```

VII. MATHEMATICAL MODEL

1) At Sender Timestamp (T_s) is calculated for each sending packet
- Where P_i are sending packet
- Timestamp (T_s) - Time at which packet send.

2) Calculate Time stamp (T_r) for each receiving packet
- And R_i are the Receiving packet
- Timestamp (T_r) - Time at which packets are received.

3) Threshold is calculated for jamming detection.
4) Calculate Threshold:

Where, T_d and T_s are the time stamps for all packets at receiver and sender respectively.

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

VIII. CONTRIBUTION AND RESULT ANALYSIS

A. 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.

B. 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. For jamming attack detection, we are using a VCM based approach for to detect whether network is jammed or not.

C. Data Access:

This module provides permit or deny 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. For accessing the data of user here we used Memory Data Access Control Policy which maintains a matrix of user and files with the user rights for to access the particular file. In MDACP, every user is connected with a key (e.g., a prime number) and every file is associated with a lock value. For each and every file, there are some consistent locks, which can be removed from prime factorization. Through simple computations on the basis of keys and locks, protected memory data can be retrieved. Access right matrix consists of number of users entry, files entry and access modes. Matrix contains different types of access modes for eg. 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.

D. Experimental Setup

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

1. Sender

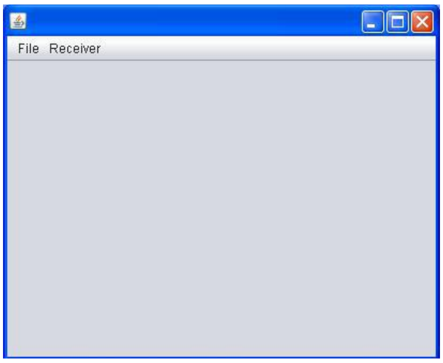


Fig 2: File Browsing

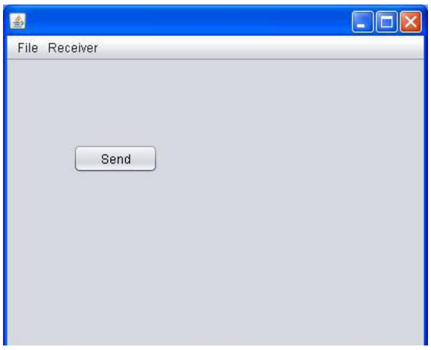


Fig 3: Sending

2. Hacker

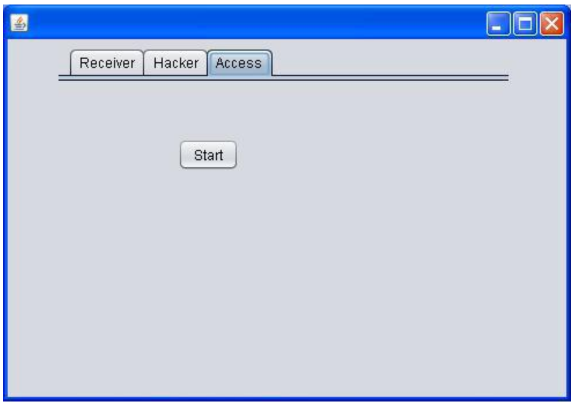
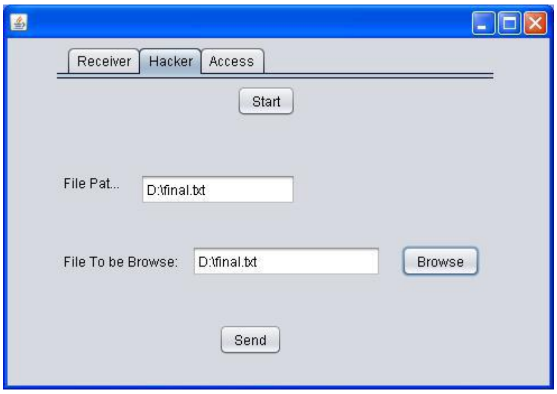


Fig 4: Access



File Pat... D:\final.txt

File To be Browse: D:\final.txt

Fig 5: Hacker

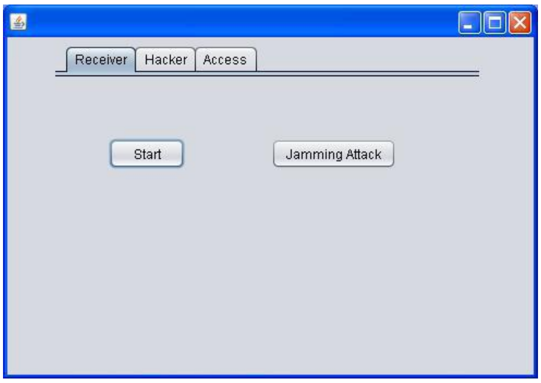


Fig 6: Receiver

3. Receiver

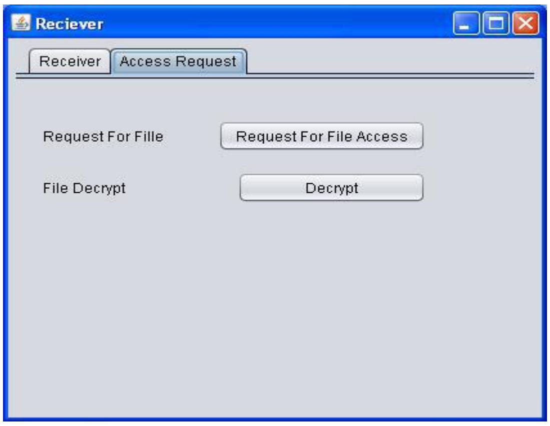
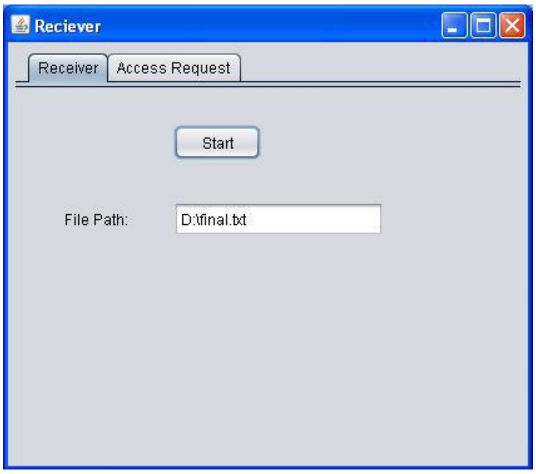


Fig 7: Access Request



File Path: D:\final.txt

Fig 8: Receiver

IX. CONCLUSION AND FUTURE SCOPE

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. Motesec-Aware is an efficient network layer security system also the security is increased by using access control mechanism. Motesec-Aware is ready to achieve to the goals of considerably less energy consumption and higher security than previous works. This helps to use the proposed implementation on any operating system and for Future work, we can find the actual source of attack from where the replay and jamming attack is happening.

ACKNOWLEDGMENT

We take this golden opportunity to owe our deep sense of gratitude to our project guide **Prof.U.H.Wanaskar**, for her instinct help and valuable guidance with a lot of encouragement throughout this paper work, right from selection of topic work up to its completion. Our sincere thanks to Head of the Department of Computer Engineering **Prof. N.D. Kale** who continuously motivated and guided us for completion of this paper. I am also thankful to all teaching and non-teaching staff members, for their valuable suggestions and valuable co-operation for partially completion of this work. We specially thank to those who helped us directly-indirectly in completion of this work successfully.

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, and Sy-Yen Kuo, “A Constrained Function Based Message Authentication Scheme for Sensor Networks” IEEE Communications Society.

DOI 10.17148/IJARCCE.2016.55167

[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]. Devesh Jinwala, Dhiren Patel and Kankar Dasgupta, "FlexiSec: A Configurable Link Layer Security Architecture for Wireless Sensor Networks" Journal of Information Assurance and Security 4 (2009) 582- 603.

DOI 10.17148/IJARCCE.2016.55167