RESEARCH ARTICLE OPEN ACCESS

Provide Practical Security Mechanism to Wireless Sensor Networks Using Modified Motesec Protocol

Monali Madne[1], Prof Manjusha Yeola[2]
1(Computer Department, University of pune, Pune)
2 (Computer Department, University of pune, Pune)

Abstract:

Wireless Sensor Network (WSN) is a promising field for research. As the use of this field increases, it is required to give proper security to this field. So to ensure the security of communication of data or messages and to control the use of data in WSN is of great importance. As sensor networks interact with responsive data and operate in unfriendly unattended area, from the time of system design these security concerns should be addressed. The paper, presents a modified Motesec security protocol which is a security mechanism for Wireless sensor network. In this protocol a hash function based approach is used to detect replay attacks. For data access control key lock matching method i.e. memory data access control policy is used to prevent unauthorized data access. Encoding and reconstruction scheme is used to find out attacker. Flooding attack detection by comparing data rate. There is currently massive research is present in the area of wireless sensor network security..Keywords: GPS,GCM,LBS Android.

Keywords: secure communication architecture, wireless Sensor network security.

I. INTRODUCTION

A wireless sensor network (WSN) is an emerging technology that consists of spatially distributed sensor nodes which cooperatively pass their collected data through the network to a main server location. Wireless Sensor Networks are consist of heterogeneous systems which contain many no of small devices called sensor nodes and actuators with general-purpose computing elements required for computation pupose.These wireless sensor networks consist of thousands or many number of sensor nodes having low power, low cost and self-organizing sensor nodes which are highly distributed either inside the whole system or very close to that system. As these nodes are highly dispersed network security is strongly required. These sensor networks consist of sensor nodes ranging from few to hundreds or even up to thousands. These nodes connected to one or sometimes may be more than one neighbor nodes.

These sensor nodes mainly consist of three main components- data processing unit, sensing unit and communication unit, additionally also consist of Two units called, base station unit and aggregation unit .From these units Aggregation unit collects data from different neighbouring sensor nodes, It then integrates all these collected data and then forwards it to the main base station unit for further processing. There are various applications of Wireless sensor networks which includes wildlife and ocean monitoring ,monitoring of manufactured machinery, safety of building , monitoring disasters like earthquake, environmental observation , applications in military logistics and manufacturing , in the forecast systems, in the applications related to health, home and office and in a various smart and intelligent systems. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. In wireless sensor network sensor node consist of several parts: such as energy source, it is usually a battery source, radio transceiver which has an internal antenna or connection to the external antenna, a microcontroller which is an electronic circuit for the communication with the sensors. These sensor nodes may have different size. The cost of sensor nodes may vary, it may ranges from a few to hundreds or thousands of dollars, it is solely depends on the complexity of the individual sensor nodes. Variation in size and cost of sensor nodes

result in corresponding variation of resources such as energy, memory, communication bandwidth, computational speed. The topology of network for wireless sensor networks may vary from a simple ring or star network to advanced multi-hop wireless mesh network.

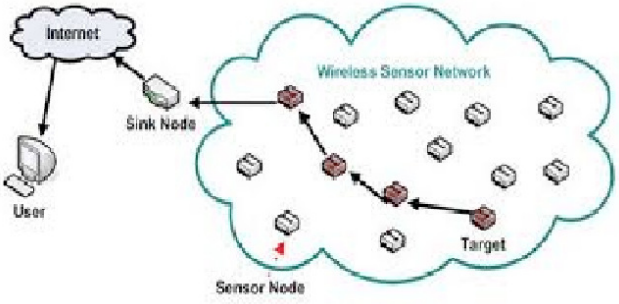


Fig 1. Wireless sensor network

II LITERATURE SURVEY

There are many methods has been proposed to secure wireless sensor networks. Review of these methods is presented as below:

Chun-Shien Lu and Yao-Tung Tsou [1] describes a security protocol called MoteSec-Aware works on a network layer .In the MoteSec-Aware, to detect replay and jamming attacks a Virtual Counter Manager (VCM) with a synchronized incremental counter is Developed which is based on the symmetric key cryptography using AES in OCB mode this cryptography technique has some drawbacks after converting plaintext into cipher text sometimes it does not retain in its original form. For data access control, they used the Key-Lock Matching (KLM) method..In this paper they implement MoteSec-Aware protocol for the TelosB prototype sensor node platform which running TinyOS 1.1.15 operating system, and they conduct field experiments and TOSSIM-based simulations to estimate the performance of MoteSec-Aware. The results shows that MoteSec-Aware consumes much less energy, yet achieves higher security than several state-of-the-art methods. MoteSec-Aware is an efficient network layer security system protocol which is fully implemented security mechanism that provides protection for both outside network message and inside memory data. This security system is able to achieve the two important goals of much less energy consumption and higher security than previous works.

Adrian Perrig, victor wen ,Robert Szewczyk, J.D Tygar,David Culler[2], proposed a security protocol SPINS which is optimized for resource constrained environments and for wireless communication. SPINS security protocol consist of two major parts µTESLA and SNEP. These two units are sufficient to provide security to sensor networks. From these the SNEP unit is used to provides data freshness, data confidentiality and two way data authentication. The main problem in sensor network is to provide efficient broadcast authentication, which is the main mechanism in sensor networks. µTESLA is used to provide this broadcast authentication in the environment where there is less number of resources. They implemented the above protocol and show that they are practical even on minimum hardware.additionaly spin protocol for WSN achieves low energy consumption but on the other hand it keeps consistent counter between sender and receiver

D Wagner ,N sastry and C Karlof[3] introduce TinySec, the first fully-implemented link layer security protocol for WSN.Traditional security protocols tends to be very limited in their guarantee of security, With less no of memories, processors which are weak in processing , limited energy environment on the other hand sensor networks cannot afford this luxury. With careful design TinySec solves these extreme resource constraints. This protocol is portable to a variety of radio and hardware platforms. The result of experiment which is taken on 36 nodes shows that this is feasible and efficient and adds less than 10% of bandwidth, latency, and energy overhead. It Achieves low energy consumption but at the same time it reduces the security provided to sensor network.

V gligor ,A.Perrig ,GMezzeour, M luk[4], proposed a protocol MiniSec it is general purpose security protocol for telos platform. it has two operating modes one which is for single source communication and other is for multisource broadcast communication. It achieves low energy consumption than tinysec and zigbee which are security protocols for WSN.and provides three important properties of secure communication secrecy, authentication and message replay protection. It uses OCB mode of encryption which is faster than CBC MAC mode.

Eduardo S.Biagioni,Galen Sasaki[5] presents and analyzes a variety of regular deployment topologies, including circular and star deployments as well as deployments in square, triangular, and hexagonal grids. In this paper, they focus on optimal strategies for placing sensor units. Individual sensor units must be placed close enough to each other that wireless communication is possible, and must be arranged so they form a network to relay data back to data collection points. In addition, nodes can be prone to failure due to events such as loss of power, operating system bugs, and equipment glitches. It is important that the network provide reliable communication that can survive node outages. A second constraint is that units must be placed so as to observe events of interest. Finally, financial or other considerations usually limit the number of units that can be deployed to study a given Area.

.

III. OVERVIEW OF PROPOSED METHOD

Addressing the constraints of low resources of sensor nodes it is planned to build Motesec Aware protocol at the network layer. As shown in Fig 2 The proposed model consist of five modules module:1.Encryption and decryption ,module:2 Replay packet detection and packet filtering ,module:3 Memory data access control ,module:4.Attacker detection and module 5 .Flooding attack detection.

Remaining paper is organized as, section IV gives the details of proposed methodology and finally section V concludes the paper.

IV. PROPOSED METHODOLOGY

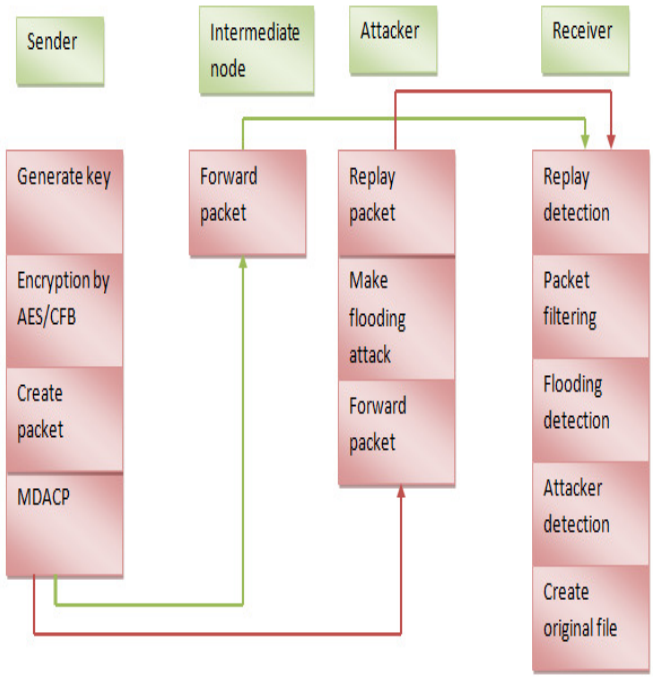


Fig 2 System architecture of proposed system

A Replay packet detection and packet filtering

In this methodology we are using two data structures Filter array and buffer which is used for probabilistic membership test and space overhead problem. It uses number of hash function and their output to check the Set membership on large size datasets. Data structure buffer consist of N size vector which consist of, Addressable cells = {a1; a2; a3; a4} and Hash functions = {h1; h2; h3; h4}. At start data structure is empty where all addressable bits are set to 0. All hash function (hj) are applied on all data (di). For replay detection, we are calculating hash of each packet. If the buffer is empty then put calculated hash on buffer if not then check the calculated hash value with value present in buffer if match found set the flag. If flag set put that hash value in the filter array data structure.All the values in filter array are discarded and the packets present in buffer are only forwarded to next node.Following algorithm is used for replay detection and for filtering of duplicate packets.

B Attacker detection

In attacker detection approach we are using header's field Type of service which is of 8 bit and identification which is of 16 bit to put the marking data D .Marking data D consist of three things first part of IP address(p),second Digest (D) and third sequence no (s).

Part of Ip Address(p)-as in 24 bit field we cant put 32 bit ip address.so we are dividing it in parts and that part is nothing but p.

Digest (D)-For all the packets coming from same source Digest field is same .unique digest is allocated to all nodes.

Sequence no(s)-at the receiver to put packet in sequence sequence no is used

C Memory Data Access Control Policy

In order to efficiently secure information in storage and defend against unauthorized users accessing data, KLM is constructed to realize MDACP In the network, personal information, key materials, and other information that have security concerns will be encrypted by AES-OCFA and stored in the inside memory.

In MDACP, each user is associated with a key (e.g. a prime number) and each file is associated with a lock value. For each file, there are some corresponding locks, which can be extracted from prime factorization. Through simple computations on the basis of keys and locks, protected memory data can be accessed.MDACP not only stores encrypted files in nodes but also binds the user keys and specific encrypted files together. This approach has greatly reduced the risk of cracking the keys by attacking the encrypted files. In addition, by employing the KLM method, whenever a new user or file is joined, the corresponding key values and lock values will be determined immediately without changing any previously defined keys and locks.

Algorithm : MDAC

Input: Key value *Ki* of user *Ui* and lock value *Lj* of file

Fj ; $1 \leq i \leq m$ and $1 \leq j \leq n$.

Output: Access rights *rij* 's.

1 Set *rij* = 0 and *Temp*= *Lj*.

2 Calculate *Q* = *Temp/Ki*. If *Q* is an integer, set

rij = *rij* + 1, *Temp* = *Q*, repeat this step until *Q* is not an integer or *rij* = *rmax*, where *rmax* is the maximum of access right.

3 Output access right *rij* .

4 If *rij*=*Yij* , then execute designate tasks and retrieve corresponding files from the memory; else reject the request.

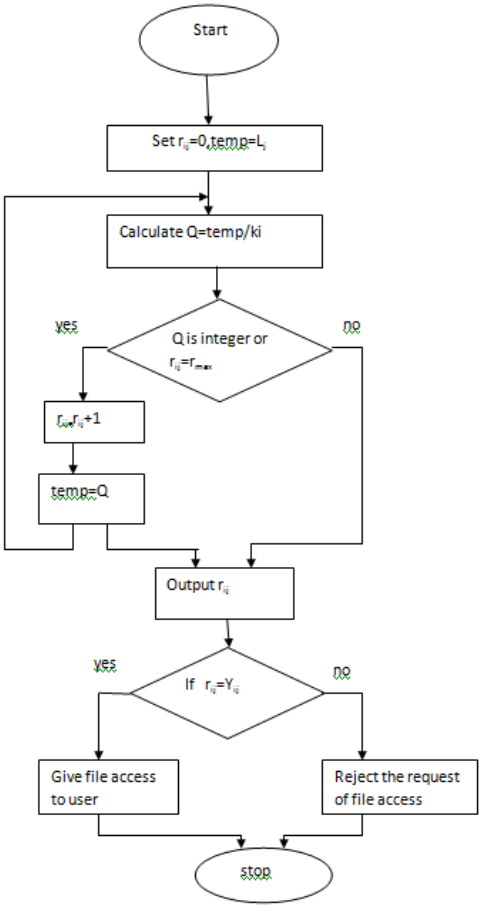


Fig 3 Data Access Control using KLM

D Flooding attack detection

In flooding attack detection at receiver end we are calculating data rate for packets received at receiver .and comparing this data rate with threshold data rate if it is greater then flooding attack is detected and receiver will automatically get stoped.it will not further receive the packets. Following algorithm is used for flooding detection

Step 1: Receive all incoming packets

Step 2: calculate current incoming packet rate by formula

$$\text{PacketRate} = \frac{\textit{No of packet receiving}}{\textit{Total Time}}$$

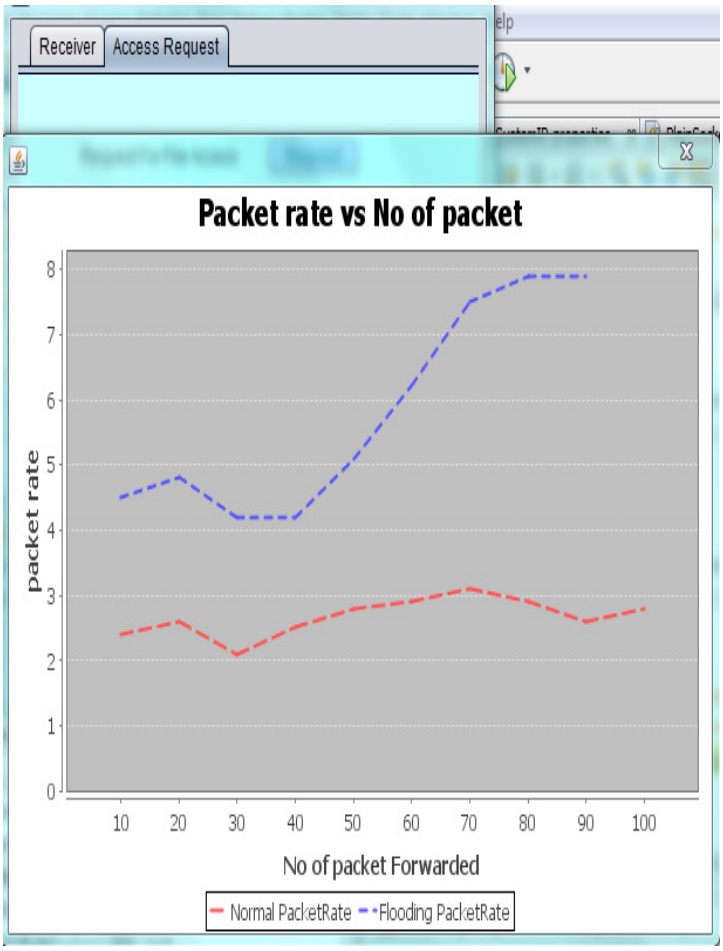
Step 3: compare the current packetrate with threshold

Step 4: if(packetRate > Threshold)

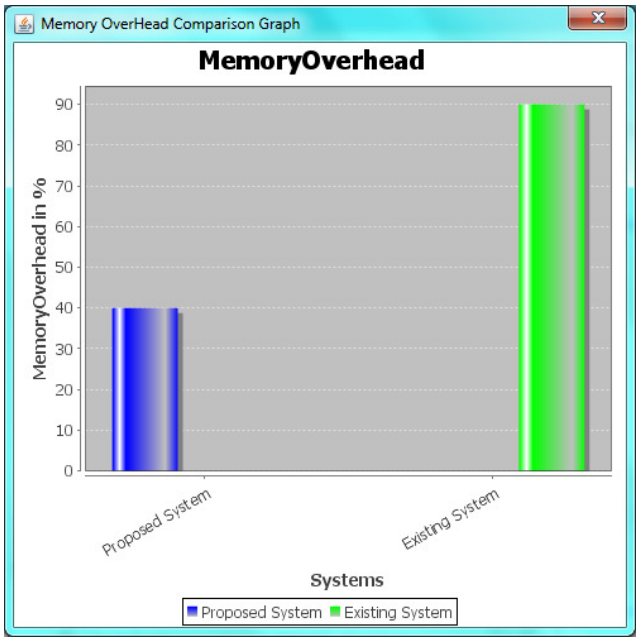
Step 5: Flooding attack Detected

Step 6: end If.

V.ANALYSIS



Graph1 . Packet rate after flooding attack



Graph2 .Memory Overhead

VI.CONCLUSION

Proposed a system which is designed to meet the goals stated below:
Propose a protocol built on network layer that focuses on data access control and secure network protocols simultaneously .Achieves lower energy consumption during communication and satisfies a high level of security without appending any additional information. Achieves replay attack detection and packet filtering with minimum storage overhead.Achieves network data security by memory data access control policy. Achieves flooding attack detection by calculating packet data rate. Achieves attacker detection by encoding and reconstruction scheme.

ACKNOWLEDGEMENT

I express my sincere and profound thanks to **Prof. Manjusha Yeola** my project guide, who always stood as the helping and guiding support for me throughout the delivery of this work. And I am thankful to all who have directly or indirectly guided and helped me in delivery of this work. Authors highly appreciate constructive comments and suggestions from reviewers to improve quality of this paper.

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] A.Perrig,R.Szewczyk, V.Wen ,D.Culler and J.D.Tygar, "SPINS:security protocol for sensor nework" ,2001 *International Conference On Mobile Computing and Networking*

[3] Chris Karlof,Naveen Sastry,David Wagner,"**TinySec: A Link Layer Security Architecture for WSN"**,2004

[4] Mark Luk ,Ghita Mezzour,Adrian Perrig,Virgil Gligor,**"MiniSec: A secure Sensor Network Communication Architecture" ,***IPSN*,April 2007.

[5] Edoardo S.Biagioni,Galen Sasaki**,"Wireless Sensor Placement For Reliable and Efficient Data Collection"**,Hawaii International Conference on System Sciences,2002

[6] Aashima Singla,Ratika Sachdeva," Review on Security Issues and Attacks in Wireless Sensor Networks",*IJARCSSE*,Vol 3,Issue 4,2013

[7] Fasee Ullah,Tahir Mehmood,Masood Habib,Muhammad Ibrahim,Shaheed Zulfikar,"SPINS:Security Protocol for Sensor Networks"**,***IPCSIT* vol3 ,2011

[8] Al-Sakib Khan Pathan,Hyung-Woo Lee,Choong Seon Hong**,"Security in Wireless Sensor Networks: Issues and Challenges"**,ICACT 2006.

[9] Deborah Estrin,Ramesh Govindan,John Heidemann,Satish Kumar,"Next Century Challenges: Scalable Coordination in Sensor Networks"

[10] Yazeed Al-Obaisat,Robin Braun,**"** On Wireless Sensor Networks: Architectures, Protocols, Applications, and Management"

[11] Ning Xu ,"A Survey of Sensor Network Applications"

[12] Mihaela cardei,Ding zhu du "ImprovingWireless Sensor Network Lifetime through PowerAware Organization"

[13] Ian F Akyildiz,Erich P stuntebeck ,"Wireless underground sensor networks:
Research challenges",2006

[14] John paul,walters,zhengqiang liang,weisong shi ,vipin choudhary," Wireless Sensor Network Security: A Survey",2006

[15] Gianluca dini & macro tiloca," Considerations on Security in ZigBee Networks",2010

[16] Amar rasheed ,Rabi N Mahapatra,"The Three-Tier security scheme in wireless sensor networks with mobile sinks",2012