ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Efficient and Trustworthy Data Transmission over Wireless Sensor Networks

Girijalaxmi[1], Mr.Vasudev S[2]

M.Tech Scholar, Department of Computer Science, Alvas Institute of Engineering and Technology,
Moodbidri, Karnataka, India[1]

Senior Assistant Professor, Department of Computer Science, Alvas Institute of Engineering and Technology,
Moodbidri, Karnataka, India[2]

Abstract: In the past few years trustworthy transmission of data along with efficiency is a critical issue for wireless sensor networks (WSNs). Clustering is an effectual and convenient way to enhance performance of the WSNs system. This thesis presents a secure transmission of data for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and sporadically. By making use of two Efficient and Trustworthy data Transmission (ETT) protocols for CWSNs, called ETT-IBS and ETT-IBOOS, by means of the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, correspondingly. In ETT-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing area. ETT-IBOOS additionally decreases the computational operating cost for protocol security, which is critical for WSNs, while its defence depends on the stability of the problem of discrete logarithm.

Keywords: Cluster-based WSN, Cluster-Head, ID-based digital signature, ID-based online/offline digital signature.

I. INTRODUCTION

A wireless sensor network is a network system it compromises the spatially distributed devices using wireless sensor nodes to examine the physical and environmental conditions such as movement, sound and temperature. In a wireless sensor network, the individual nodes are competent of sensing, processing and communicating data from one point to another point through a wireless link. In cluster based wireless sensor networks many sensor systems are deployed in harsh, and often adversarial physical environments, such as battle fields and military domains with trust less surroundings. Trustworthy data transmission is most crucial issues for wireless sensor networks. So that secure and trustworthy data transmission is needed and demanded in many practical wireless sensor networks.

II. LITERATURE SURVEY

These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Security is therefore important in WSNs. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and the use of insecure wireless communication channels. These constraints make security in WSNs a challenge. This article presents a survey of security issues in WSNs. Firstly outlined the constraints, security requirements, and attacks with their corresponding countermeasures in WSNs then presented a holistic view of security issues. These issues are classified into five categories: cryptography, key management, secure routing, secure data aggregation, and intrusion detection.

The Limitations of this paper was security services certainly add more computation, communication and storage cost in WSNs, and thus consume more energy.

A.Manjeshwar *et al* [2].Has discussed wireless sensor networks are a new class of Ad Hoc networks that will find increasing deployment in coming years, as they enable reliable monitoring and analysis of unfamiliar and untested environments. The advances in technology have made it possible to have extremely small, low powered sensor devices equipped with programmable computing, multiple parameter sensing, and wireless communication capability. But, because of their inherent limitations, the protocols designed for such sensor networks must efficiently use both limited bandwidth and battery energy. In this paper, developed an M/G/1 model to analytically determine the delay incurred in handling various types of queries using the enhanced APTEEN (Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network protocol) protocol and this protocol uses an enhanced TDMA schedule to efficiently incorporate query handling, with a queuing mechanism for heavy loads. It also provides the additional flexibility of querying the network through any node in the network. To verify analytical results, with a Poisson arrival rate for queries on the network simulator ns2. As the simulation and analytical

Copyright to IJIREEICE
DOI 10.17148/IJIREEICE

results match perfectly well, this can be said to be the first step towards analytically determining the delay characteristics of a wireless sensor network.

The Disadvantage of this paper was delay in answering the query is greatly depends on the frame length and Additional complexity is required to implement the threshold functions, the count time and the query handling at the nodes.

R. Yasmin *et al* [3].Has pointed that in Wireless Sensor Networks (WSNs), authentication is a crucial security requirement to avoid attacks against secure communication, and to mitigate against DoS attacks exploiting the limited resources of sensor nodes. Resource constraints of sensor nodes are hurdles in applying strong public key cryptographic based mechanisms in WSNs. To address the problem of authentication in WSNs, R.yasmin has proposed an efficient and secure framework for authenticated broadcast/multicast by sensor nodes as well as for outside user authentication, which utilizes identity based cryptography and online/offline signature (OOS) schemes. The primary goals of this framework are to enable all sensor nodes in the network, firstly, to broadcast and/or multicast an authenticated message quickly; secondly, to verify the broadcast/multicast message sender and the message contents; and finally, to verify the legitimacy of an outside user.

The Disadvantage of this paper was Computation cost is more that is generating and verifying the signature cost and the usage of memory is more.

H. Lu *et al* [4].Has explained the secure routing for cluster based sensor networks where clusters are formed dynamically and periodically. And pointed out the deficiency in the secure routing protocols with symmetric key pairing. Along with the investigation of ID-based cryptography for security in WSNs, a new secure routing protocol with ID-based signature scheme has proposed for cluster-based WSNs, in which the security relies on the hardness of the Diffie-Hellman problem in the random oracle model. Because of the communication overhead for security, this paper provides analysis and simulation results in details to illustrate how various parameters act between security and energy efficiency.

The Disadvantages of this paper was the proposed protocol requires the extra energy consumption for computation and still security overhead is more.

III. PROBLEM STATEMENT

A. Network Design

Let us consider a CWSN consisting of a preset base station (BS) and a large number of wireless sensor nodes, which are uniform in functionalities and capabilities. We presume that the BS is always reliable, i.e., the BS is a trusted entity. In the meantime, the sensor nodes may be compromised by external attackers, and the transmission of data may be interrupted from attacks on wireless channel. In a CWSN, sensor nodes are assembles into cluster, and every cluster has a cluster-head (CH) sensor node, which is chosen separately. Leaf sensor nodes which are non-CH nodes join a cluster depending on the receiving signal power and transmit the sensed data to the BS through CHs to save energy. The CHs perform data fusion and transmit data to the BS straight away with reasonably high energy. We presume that, all sensor nodes and the BS are time synchronized with symmetric radio channels, nodes are disseminated arbitrarily, and their energy is controlled.

During data sensing, processing and communication in CWSN, energy of sensor nodes is consumed. The cost of data transmission is more than that of data processing. Thus, the technique that the intermediary node (i.e, a CH) aggregates data and sends it to the BS is preferred then the technique that every sensor node directly sends to the BS. A sensor node goes to sleep node for power savings. When it does not sense or transmit data and it depending on the TDMA (time division multiple access) control used for transmission of data.

B. Security Vulnerabilities and Protocol Goals

The cluster based protocol (like LEACH) which are data transmission protocol for WSNs, are vulnerable to a many security attacks. In general, the attacks to CHs in CWSNs could produce a serious damage to the network, since data aggregation and data transmission rely on the CHs fundamentally. If an attacker manages to act as if it's a CH or negotiate the CH, it can provoke attacks such as sinkhole and selective forwarding attacks, thus upsetting the network. Alternatively an attacker may intend to inject false sensing data into the WSN like pretending as a leaf node to transform the bogus information to the CHs. However, LEACH like protocols are tougher against insider attacks rather than other types of protocols in WSNs. Since CHs are rotating from nodes to nodes in the network by rounds making it harder for external attackers to recognize the routing fundamentals as the intermediary nodes and attacks them. The properties in LEACH like decrease the risk of being attacked on intermediary nodes, and make it difficult for an external attacker to recognize and compromise important nodes. The aim of the proposed efficient and trustworthy data transmission for WSNs is to guarantee an efficient and trustworthy transmission of data between leaf nodes and the CHs, as well as transmission between CHs and BS by using ID-based digital signature and ID-based offline/online digital signature protocols.

IV. EXISTING SYSTEM

In a Wireless sensor networks(WSNs) many WSNs are deployed in harsh, neglected and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trust less surroundings. Wireless sensor network comprised of

DOI 10.17148/IJIREEICE

spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and movement.

The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN. This is the type node compromising attack and other types of attacks like active and passive attacks occur while exchanging the packets between the nodes.

V. PROPOSED SYSTEM

In this Proposed System, Efficient and Trustworthy data transmission is thus especially necessary and is demanded in many such practical wireless sensor networks.

So, two Efficient and Trustworthy data Transmission protocols for Cluster based wireless sensor networks, called ETT-IBS and ETT-IBOOS are proposed, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively.

Protocols are proposed in order to reduce the computation and storage costs to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.

In the proposed protocols pairing parameters are distributed and preloaded in all sensor nodes by the BS initially

VI. SYSTEM DESIGN

UML Stands for Unified Modelling Language. UML is a standard language for specifying, visualizing, constructing, and documenting the artifacts of software system.

In this section, the emphasis given on the explanation of architecture of design and use case diagram and data flow diagram.

A. System Architecture

Work flow of ETT-IBS Protocol and its Operation: Efficient communication in ETT-IBS relies on ID based cryptography in which user public keys are their ID information.

Thus, users can obtain their private keys without auxiliary data transmission, which is efficient in communication and saves energy. Fig 1 illustrates the process of encryption and decryption using the keys generated.

As shown in fig private key is generated from nodes ID and the master key (msk) function of Base station (BS). Similarly, public key is generated from master key function of CH. Using these keys security can be provided to the data.

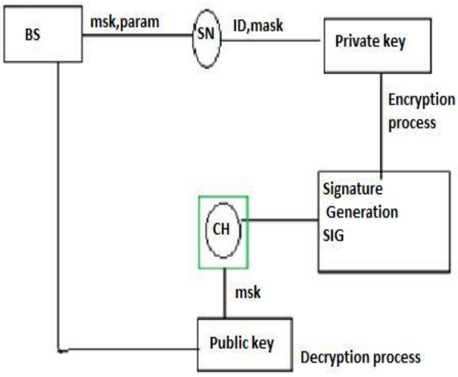

Fig 1: Work flow of ETT-IBS protocol

Work flow of ETT-IBOOS and its Operation: ETT-IBOOS is proposed in order to further decrease the computational overhead for security using the IBOOS scheme, in which security relies on the hardness of the discrete logarithmic problem.

Private Key is generated in similar way as that of IBS, Along with private key online signature is generated for encrypting the data. This online signature is obtained using offline signature.

While decrypting the data online signature, sensor node ID and message M parameters are used as shown in Fig 2.

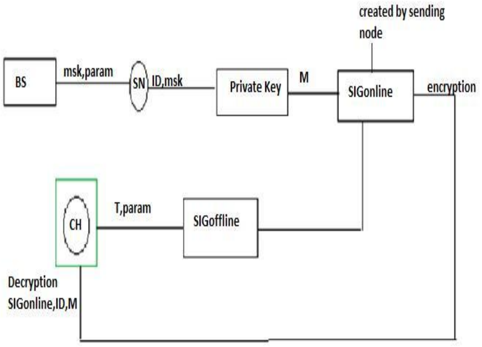

Fig 2: Work flow of ETT-IBOOS protocol

A. Use case Diagram

A use case illustrates a unit of functionality provided by the system. Fig 3 shows the workflow of the use case diagram. Initially the sender will browse the encrypted file and initializes the MAC address to all the sensor nodes using the AES and SHA1 algorithms and upload file to router. Router will find the all possible shortest paths to route the data if attack is found then it will send attacker details to router and the sender and to overcome the attack IBS protocol is used to take the alternative route to transforms the file to destination. if there is no attack then router will forward the file to receiver. Receiver receives the file/data and checks the digital signature and decrypt the file.

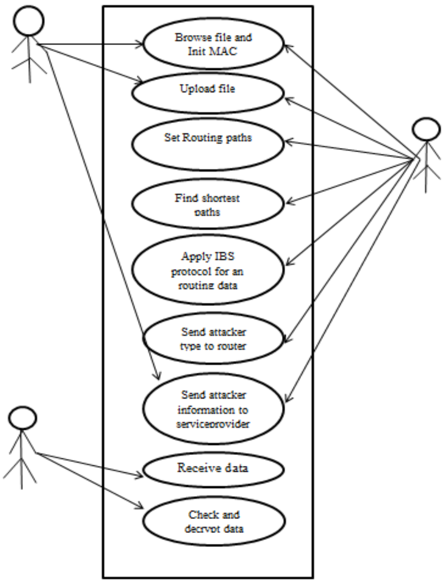
Browse file and Init MAC
Upload file
Set Routing paths
Find shortest paths
Apply IBS protocol for an routing data
Send attacker type to router
Send attacker information to serviceprovider
Receive data
Check and decrypt data

Fig 3: Use Case Diagram

A. *Data Flow Diagram*

The Data Flow Diagram provides a graphical representation of the flow of data through a system. It shows logically what information is exchanged by our system processes and external interfaces or data stores, but it does not explicitly show wen or in what sequence the information is exchanged. Fig 4 shows the work flow of the data flow diagram. Sender browses the files and initializes the message authentication code to every sensor nodes and upload file to the router. Router finds the shortest paths to forward file to the receiver/destination if there is no attack. If there is a attack then it sends attacker details to router and to overcome the attacks applies the decision making techniques by using the IBS protocol to resend data from sender through alternative routing paths else file or data will discarded.

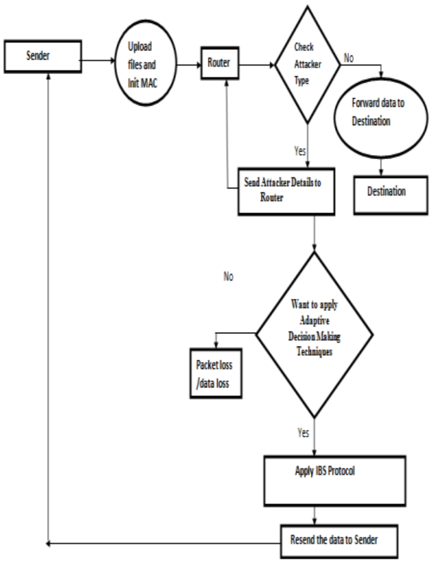
Sender
Upload files and Init MAC
Router
Check Attacker Type
No
Forward data to Destination
Yes
Send Attacker Details to Router
Destination
No
Want to apply Adaptive Decision Making Techniques
Packet loss /data loss
Yes
Apply IBS Protocol
Resend the data to Sender

Fig 4:Data Flow Diagram

VII. ALGORITHMS

- AES (Advanced Encryption Standard) algorithm is used for the file encryption and the decryption.
- SHA-1(Secure hash algorithm) algorithm is used for online/offline digital signature (MAC Message Authentication Code),ID Based Digital Signature.

VIII. APPLICATIONS

- Using in wide area network computing to enhance the throughput of the entire network.
- This is applicable in military and delay tolerant networks.
- The system is applicable in Hierarchical Clustered Wireless Sensor Networks also.

REFERENCES

[1]. Y.Wang, G. Attebury, and B.Ramamurty,"A Survey of Security Issues in Wireless Sensor Networks," IEEE Commun. Surveys Tuts.,vol.8, no. 2, 2006.

[2]. A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, "An analytical model for infor-mation retrieval in wireless sensor networks using enhanced APTEEN protocol," IEEE Trans. Parallel Distrib. Syst., vol. 13, 2002.

[3]. R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures," in Proc. IEEE CIT, 2010.

[4]. H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-based Wireless Sensor Networks Using ID-based Digital Signature," in Proc. IEEE GLOBCOM, 2010.

[5]. L. B. Oliveira, A. Ferreira, M. A. Vilac¸a et al., "SecLEACH-On the security of clustered sensor networks," Signal Process., vol. 87, pp. 2882–2895, 2007.

[6]. Nikolaos A. Pantazis, Stefanos A.Nikolidakis, Dimitrios D.Vergados,"Energy-Efficient Routing Protocols in Wireless Sensor Networks", A Survey IEEE Communications surveys & tutorials, vol. 15, no. 2, second quarter 2013

DOI 10.17148/IJIREEICE