ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

SECURE AND EFFICIENT WATCHDOG OPTIMIZATION FOR CLUSTER BASED WIRELESS SENSOR NETWORKS

(T.PARUVATHAVARTHINI(AP/ECE), P.LAVANYA(711212106049), G.NAGAJOTHI(711212106058), A.NANDHINI(711212106058)

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING, JAY SHRIRAM GROUP OF INSTITUTIONS, AVINASHIPALAYAM, TIRUPUR.

ABSTRACT

Watchdog technique is a fundamental building block to many trust systems that are designed for securing wireless sensor networks (WSNs). Unfortunately, this kind of technique consumes much energy and hence largely limits the lifespan of WSN. It reveal the inefficient use of watchdog technique in existing trust systems. To overcome this drawback, this paper propose a suite of optimization methods to minimize the energy cost of watchdog usage, while keeping the system security in a sufficient level. Here we propose secure and efficient data transmission (SET) protocol for CWSNs, called SET IBS, by using the Identity Based digital Signature (IBS). In SET IBS, security release on the hardness of the Diffie-Hellman in pairing domain. The calculations and simulations are provided to illustrate the efficiency of the Dynamic Source Routing protocol(DSR). The results show that, the proposed protocols (SET-IBS) have the better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

KEYWORDS

Clustering, digital signature, Dynamic Source Routing, SET-IBS.

INTRODUCTION

The wireless sensor network consist of small sized,light weighted, low power, inexpensive wireless nodes called sensor nodes, deployed in physical or environmental condition. And it is measured physical parameters such as sound,temperature,pressure,humidity and light. In WSNs the individual sensor nodes are capable of data sensing their environments,processing the data locally,sending data to one or more collection points and aggregates the data and sends the data to the base station in WSN as shown in fig1.the cost of data transmission is much more expensive than that of data processing. The sensor nodes have the ability to communicate either among each

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

other or directly to a base station. Data in sensor networks are bound either downstream to nodes from a sink node or upstream to sink node from nodes. Wireless sensor networks are a kind application specified network.

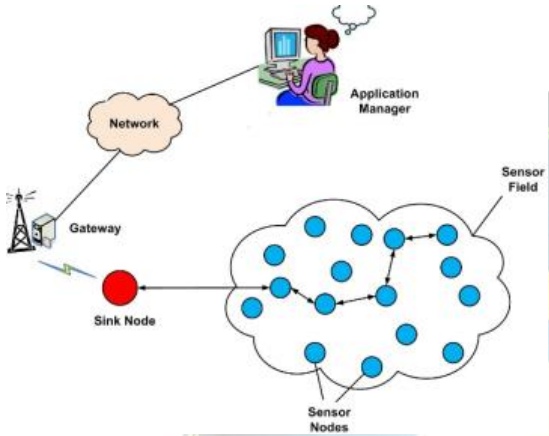


Fig1.wireless sensor network

RELATED WORK

Security in wireless sensor networks

Wireless sensor network applications include ocean and wildlife monitoring, manufacturing machinery performance monitoring, building safety and earthquake monitoring, many military applications. An even wider spectrum of future application is likely to follow, including the monitoring of highway traffic, pollution, wildfires, building security, water quality and even peoples heart rates. A major benefits of this system is that they performing network processing to reduce the larges streams of raw data into useful aggregate information.

Two factor user authentication in wireless sensor networks

Wireless sensor networks are typically deployed in an unattended environment, where the legitimate users can login to the network and access data as and when demanded. Consequently, authentication is a primary concern in this resource constrained environment before accessing data from the sensor /gateway nodes. We present two factor user authentication protocol for WSN,which provides strong authentication, session key establishment and achieves efficiency or sensor node.

Access control in wireless sensor networks

Nodes in a sensor networks may be lost due to power exhaustion or malicious attack. To extend the life time of the sensor network,new node deployment is necessary. In military scenarios, adversaries may directly deploy malicious nodes or manipulate existing nodes to introduce malicious “new” nodes through many kinds of attacks. To prevent malicious nodes from joining the sensor network,access control is required in the design of sensor network protocols. In this paper,we propose a access control protocol based on elliptic curve cryptography(ECC) for sensor network. Our access control protocol accomplishes node authentication and key establishment for new nodes. Different from conventional authentication methods based on the node identity, our access control protocol includes both the node identity and the node

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

bootstrapping time into the authentication procedure.

Mitigating routing misbehavior in mobile ad-hoc networks

In this way, we can make only minimal changes to the underlying routing algorithm. We introduce two extensions to the dynamic source routing algorithm(DSR) to mitigate the effects of routing misbehaviors: the watchdog and the pathrater. The watchdog identifies misbehaving nodes, while the pathrater avoids routing packets through this nodes. Christo Ananth et al. [4] discussed about a method, Wireless sensor networks utilize large numbers of wireless sensor nodes to collect information from their sensing terrain. Wireless sensor nodes are battery-powered devices. Energy saving is always crucial to the lifetime of a wireless sensor network. Recently, many algorithms are proposed to tackle the energy saving problem in wireless sensor networks. There are strong needs to develop wireless sensor networks algorithms with optimization priorities biased to aspects besides energy saving. In this project, a delay-aware data collection network structure for wireless sensor networks is proposed based on Multi hop Cluster Network. The objective of the proposed network structure is to determine delays in the data collection processes. The path with minimized delay through which the data can be transmitted from source to destination is also determined. AODV protocol is used to route the data packets from the source to destination.
Pathrater described above should improve performance significantly in the case where the watchdog is not active.

Group-based trust management scheme for clustered wireless sensor networks

We propose a new light weight group based trust management scheme (GTMS) for wireless sensor networks, which employs clustering. Our approach reduces the cost of trust evaluation. Also, theoretical as well as simulation results so that so that our scheme demand less memory, energy and communication overheads as compared to the current state of the art trust management schemes and it is more suitable for large scale sensor network. In this work, we propose a new lightweight group- based trust management scheme (GTMS) for wireless sensor networks. The GTMS consist of three unique features such as GTMS evaluate the trust of a group of SNs in contrast to traditional trust management scheme that always focus on trust values of individual nodes.

EXISTING SYSTEM

This conflicts has not been comprehensively addressed by prior research in the literature. We optimize watchdog techniques in two levels, both of which consist of a theoretical analysis to show potential optimal results and a practical algorithm to efficiently schedule watchdog tasks. We evaluate our optimization techniques using extensive experiments in a WSNET simulation platform and an in-door test bed in our collaborative lab. The experimental results

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

have successfully confirmed the effectiveness of our design. Our ultimate goal is to reduce the energy cost induced by watchdog tasks as much as possible, while keeping trust accuracy and robustness in a sufficient level.

DISADVANTAGE

Inefficient us of watchdog technique.

It takes maximum energy cost for watchdog usage.

Energy sacrificing much security.

Accuracy and robustness is not in sufficient level.

METHODOLOGY:

PROPOSED SYSTEM

In this proposed system, secure and efficient data transmission is thus especially necessary and is demanded in many such practical WSNs. So, we propose secure and efficient data transmission (SET) protocol for CWSNs, called SET-IBS, by using the Identity-Based digital Signature (IBS) scheme, respectively.

It has been 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.

ADVANTAGES

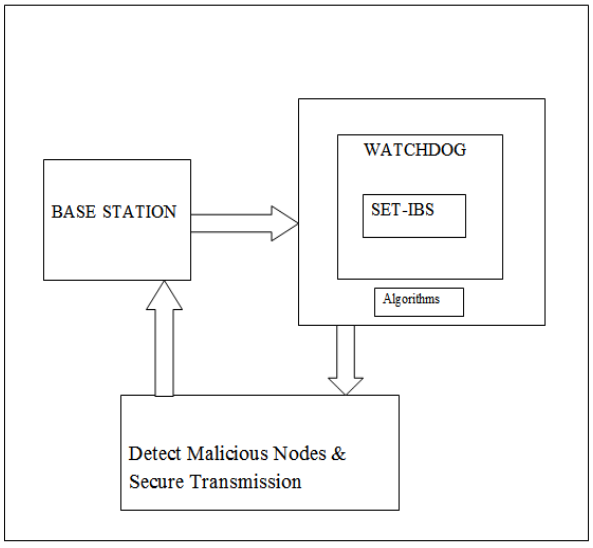
In this technique we have save more energy without sacrificing much security.

Here the trust accuracy and robustness in a sufficient level.

Efficient usage of SET-IBS technique.

Minimized energy cost and reduced energy consumption.

.



ARCHITECTURE DESIGN

MODULES DESCRIPTION

LIST OF MODULES

Cluster formation

SET protocol

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

Key management for security

Signing of signature and verification

Cluster formation

The nodes energy is the most important issue because the nodes are small in size and it may be deployed in hazardous areas, thus making battery replacement unpractical and impossible. Therefore, it is more practical to save energy and prolong the network lifetime by improving the routing algorithm. Cluster based hierarchical routing protocol is an energy efficient routing protocol. In the cluster routing, the sensor nodes will be divided into a few groups with one cluster head elected for each group. The cluster head collects data from member nodes in the same cluster and aggregates the collected data so that it can be transmitted to the base station. Implementing this protocol will significantly reduce the overall energy used and reduce the network congestion by only allowing the cluster head to communicate with the base station.

Set protocol

In this module, secure and efficient data transmission protocol for CWSNs. The protocol is designed with the same purpose and scenarios for CWSNs with higher efficiency. The proposed scheme operates similarly to the previous key management, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We first introduce the protocol initialization then describe the key management of the protocol by using the protocol operations afterwards. This method used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. The probability of neighborhood authentication, where only the nodes with the pair wise key can authenticate each other.

Key management for security

In this module, security is based on the multiplicative group. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. In this module, the key cryptographies used in the protocols to achieve secure data transmission, which consist of symmetric and asymmetric based security. This scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. It proposed an efficient key management framework to ensure isolation of the compromised nodes. It represents the requirements of the security keys stored in sensor nodes memory.

Signing of signature and verification

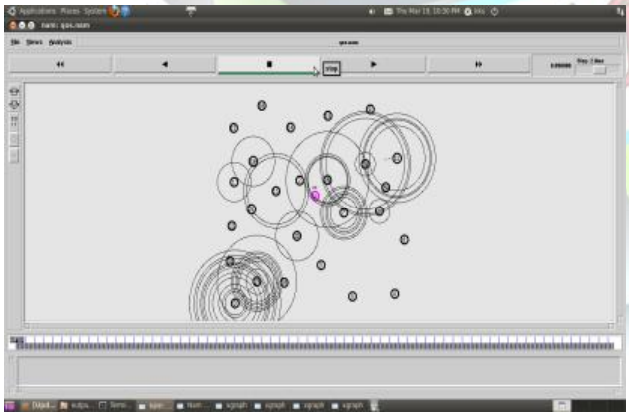
In this module, used for secure access and data transmission to nearby sensor nodes, by authenticating to each other. Each nodes have each signature to authenticate the node, sender and receiver. And key is created for every data and send

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 3, April 2016

to both receiver and the sender nodes. The signature is used for this signature generation and key generation. It checks whether the information coming from secure sender and from the correct path. After authentication,receives the information through the secure nodes. It used for secure access and data transmission to nearby sensor nodes, by authentication with each other. Here, "limited" means the probability of neighborhood authentication,where only the nodes with shared pair wise key can authenticate each other. The energy cost and computation efficiency on the generation and verification of the certificates or signatures for security.

RESULT:

Thus the simulation output of the secure and efficient optimization for cluster based wireless sensor networks is given by,



SIMULATION OUTPUT

REFERENCE

[1] T. Hara, V.I. Zadorozhny, and E.Buchmann, Wireless sensor Network Technologies for the Information Explosion Era, studies in computational Intelligence, vol.278. springer-verlag, 2010.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, 'A Survey of Security Issues in Wireless Sensor Networks,'' IEEE comm. Survey & Tutorials, vol.8, no. 2, pp. 2-23, second quarter 2006.

[3] A.A. Abbasi and M. Younis, "A Survey on clustering algorithms for Wireless Sensor Networks," Computer Comm, vol. 30, nos. 14/15, pp. 2826-2841,2007.

[4] Christo Ananth, T.Rashmi Anns, R.K.Shunmuga Priya, K.Mala, "Delay-Aware Data Collection Network Structure For WSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Special Issue 2 - November 2015, pp.17-21

[5] A. Manjeshwar, Q.-A. Zeng and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN protocol," IEEE Trans. Parallel &distributed systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.

[6] S. Yi et al, "PEACH: Power-Efficient and Adaptive clustering Hierarchy Protocol for Wireless Sensor Network," Computer Comm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.

[7] K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor

Networks." Int1J. computer Applications, vol.47, no. 11, pp. 23-28, 2012.

[8] L.B. Oliveira et a., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.

[9] P.Banerjee,D.jacobson, and S.Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Network, "Proc.IEEE Sixth Int'1 Symp. Network Computing and Application(NCA) ,pp.145-152,2007.

[10] K.Zhang, C. Wang, and C.Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Network Using Group Key Management." Proc. Fourth Int'1 Conf. Wireless Comm., Networking and Mobile Computing(WiCOM), pp.1-5,2008.