ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 15, March 2016

CRYPTOGRAPHY TECHNIQUES USED IN SECRET KEY MANAGEMENT SYSTEM IN WIRELESS SENSOR NETWORK

MR.A.VIJAY VASANTH[1]
M.E., (Ph.D) Dept. of CSE
Senior Assistant Professor
Christ College of Engineering & Technology,
Pondicherry, India

M.SHANTHINI[2]
M.Tech., Dept. of CSE
Christ College of Engineering & Technology,
Pondicherry-605110, India

P.VIDHUSHINI[3]
M.Tech., Dept. of CSE
Christ College of Engineering & Technology,
Pondicherry-605110, India

Abstract: Wireless Sensor network used to provide the Security and the Energy consumption are different concerns. This paper aim to minimize the Energy Consumption after attack which may drain the life time of the node. The Duty Cycle Protocol is based on Energy conversation for Wireless Sensor Network. The Low Power Listening based on Medium Access control protocol counter the attack in an Energy Efficiency. The Secure adaptive topology control protocol algorithm used to form hierarchical topology against power exhausting to distribution the keys to make the Energy Efficiency. This happens especially during denial of sleep attack. The Medium Access Protocol used to save the power and extend the life time wireless sensor network (WSN). The Elliptical curve cryptography using scalar multiplication technique is security mechanism to Encrypted and Decrypted the data using reverse string process. The Energy distribution key make the decision rule between the energy conservation and security requirement for wireless sensor network is used.

***Key words**: Wireless sensor network, Low Power Listening Protocol, Medium Access Protocol, Elliptical curve cryptography protocol, Secure adaptive topology control protocol.*

1. INTRODUCTION

A Wireless Sensor network consists of multiple detection stations called sensor nodes. It is used for energy efficiency, power consumption, load balancing, and power analysis. Wireless Sensor Network is used collect data form environment. It consists of large number of sensor node and one or more base stations. The network node connected in the wireless communication channels. Each node as capability to sense the data, process the data and send it to the rest of the nodes. Wireless sensor node or simply a sensor node consists of the sensing, computing, communicating and power consumption. Wireless networks of thousands of inexpensive miniature devices capable of computation, communication and sensing. A self-configuring network of small sensor nodes communicating among themselves using radio signals, and deployed in quantity to sense, monitor and understand the physical world. A Wireless Sensor network consists of spatially distributed autonomous sensors to monitor physically or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants and to cooperatively pass their data through the network the network to a main location.

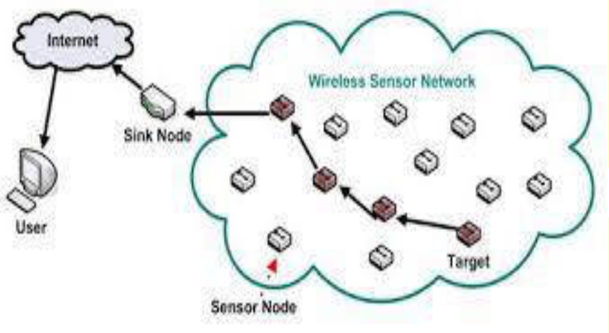

Fig. 1.1 Wireless Sensor Network

Each of the small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. Wireless Sensor Network is an application-specific technology – for example, temperature sensor nodes only measure temperature and nothing else. It is range from dense to sparse, from mobile to static.

2. RELATED WORKS

2.1 Adaptive Energy Efficient MAC Protocol for Wireless Sensor Networks

The Channel allocation is based on the request initial energy with desirable number of transmission. The Medium Access Protocol Layer propagates the utilization factors of the former node to the successor node. A contention based Medium control for wireless sensor network. The shortest path algorithm used for the node-to-sink communication is used.

The Nodes-to-Sink Communication to the nodes the Send the messages to a single sink node at the corner of the network. Messages are routed from node to node with the shortest path algorithm. So, the no data aggregation is used. For the T-MAC protocol, we used overhearing avoidance, the priority mechanism, and the FRTS mechanism.

2.2 Secure Adaptive Topology Control for Wireless Ad-Hoc Sensor Networks

Depending upon nodes transmission energy the number of communication is either increases or decreases such that minimum drops occur due to fading Lifetime of the node. A Secure decentralized clustering algorithm for wireless ad-hoc sensor networks. The algorithm operates without a centralized controller, operates asynchronously, and does not require that the location of the sensors.

Based on the cluster-based topology, secure hierarchical communication protocols and dynamic quarantine strategies are introduced to defend against spam attacks, since this type of attacks can exhaust the energy of sensor nodes and will shorten the lifetime of a sensor network.

The Secure Adaptive Distributed Topology Control Algorithm (SADTCA) aims at topology control. When the cluster head finds out the occurrence of a spam attack, it broadcasts a message throughout the whole cluster. In this condition, the set of quarantine nodes is composed of the cluster head and cluster member.

2.3 Secure Wake-Up Scheme for Wireless Sensor Network

For node remains in sleep state till it receiver the correct true packet from sender otherwise it drops packet and received the back to the sleep state. Each node (dust particle) is equipped with some sensors, an embedded processor, and a low-power radio for short-range communication. With such cheap, autonomous nodes large multi-hop, ad-hoc networks can be formed in which cooperating nodes can overcome their inherent individual limitations and provide extensive services, especially in the area of monitoring and control. The idle listening is the S-MAC protocol, a true MAC protocol, which also addresses the overheads caused by collisions, overhearing, and protocol overhead.

3. TECHNIQUES AND A PROTOCOL USED FOR DISTRIBUTED KEY MANAGEMENT SYSTEM

3.1 Low Power Listening Protocol

In the Low Power Listening (LPL) based Wireless Sensor Network Medium Access Control protocol, such as B-MAC, the receiver wakes up periodically to sense the preamble from the sender and then to receive and process the data. The Low-Power-Listening (LPL) protocols transmit packets the inter listening interval, thereby, allowing nodes to sleep for long periods of time between channel problems. When the sender needs to send data, it sends a long preamble to cover the sleep period to ensure the receiver waking up and sensing.

The Low Power Listening Protocol based Medium Access control protocol is an asynchronous protocol, which decouples the sender and receiver with time synchronization. The inter listening interval as well as particular period of time type of Low Power Listening protocol should be well matched to the network condition.

The network– aware adaptation of the specific succession of repeated packet over the U interval (the “MAC schedule”), which yield significant energy saving. Moreover, some Low Power Listening protocol interrupt communication between the sender and the receiver after the data packet has been successfully received.

We proposed new and simple adaptation of the “transmit/receive schedule” to synchronize node on a slowly changing path so that energy consumption and delay are further reduced, at no cost of overhead in most cases. Our result show that using network-aware adaptation of the MAC schedule provides up to 30 percent increases in lifetime for different traffic scenarios.

3.2 Duty cycle based Protocol

The duty cycle based protocol is one of the major schemes in energy conservation for wireless sensor network. In the duty cycle based protocol wireless Sensor network MAC protocols, sensor nodes are switched between awake/active and sleep state periodically and these nodes enter sleep mode after certain ideal period.

In the Low Power Listening based protocol Wireless Sensor network MAC protocol, such as B-Mac the receiver wakes up periodically to sense the preamble from the sender and then to receiver and process the data. When the sender needs to send data, it sent a long preamble to cover the sleep period to ensure the receiver waking up and sensing.

The Low Power Listening based MAC protocol is an asynchronous protocol, which decoupled the sender and receiver with the time synchronization. This long preamble design of LPC based protocol consumes the major energy of both sender and receiver. The sender and receiver scheme is used. The current methodology to suggest that a cross-layer design of energy-efficient secure scheme integrating the MAC protocol. No extra packet is involved in the original MAC protocol design.

This scheme can reduce the authenticating process as short as possible to mitigate the effect of the power exhausting attacks. By combination of low complexity security process and multiple check points and their design can defense against attacks and send the sensor nodes back to sleep mode as soon as possible. Depending on the different initiator, the duty-cycle scheme can be classified into two types. The sender-initiated scheme and receiver initiated (RI) scheme. For instance, the X-MAC protocol is one of the sender-initiated schemes to improve B-MAC protocol by replacing the long preamble with short preamble allows the receiver to send acknowledgment

3.3 Elliptical Curve Cryptography using Scalar Multiplication Technique

The Elliptical curve cryptography using Scalar Multiplication in an approach to public key cryptography based on algebraic structure of elliptical curve over a finite field. One of the benefits in comparison with non- Elliptical Curve Cryptography (with plain Galois fields as a basic) is the same level o security provided by keys of smaller size. Elliptic curves are applicable for encryption, digital signature, pseudo-random generators and other tasks.

They are also used in several integer factorization algorithms that have applications in cryptography, such as elliptic curve factorization a large number of cryptographic primitives based on bilinear mappings on various elliptic curve groups, such as the Weil and Tate pairing, have been introduced. Schemes based on these primitives provide efficient identity-based encryption as well as pairing-based signatures, sign encryption, key agreement, and proxy re-encryption.

We suggest that the source node broadcast the public key based request message to neighbors for establishing the path to destination. The timing attacker nodes node forwards the request message continuously to unreached destination faster than its first source neighbors, at this point source node checks it routing table and performs Elliptical curve cryptography scalar multiplication process and identifies it is a malicious node and updates its block tables that node is a malicious node.

Thus the proposed system which is having two type of attacks one is timing attack and other one is power analysis attack. The Elliptical Curve Cryptography Scalar Technique is used for used to distributed key is a security mechanism awake the sensor node to extend the life time of sensor nodes is used. A timing attack is a side channel attack in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic a

4. MODULE DESCRIPTION

4.1 Anti-Node Detection

In this module, the network formation is robust in nature against attacks, an authenticated broadcasting mechanism a plaintext “Hello” message is encrypted by the pre-distributed key as the broadcasting challenge. If the sensor cannot decrypt the received message successfully, the sender is said to be an anti-node. Thus the normal nodes and antinodes can be differentiated. Thus, we formed the network topology without anti-nodes in order to make the network safe. An external attack can be prevented by the operations. In this work, we do not have a lightweight countermeasure to defend against authenticated malicious nodes. Hence the authenticated node is compromised and performs malicious activities a mechanism for evicting the compromised nodes is required.

4.2 Cluster Formation

Cluster formation is a process of selecting the head and frames the sensor sets to be randomly waiting the timer and broadcasts “Hello packets” signal, and listens for its neighbor's "Hello packets." The sensors that hear many neighbors are good candidates for initiating new clusters; those with few neighbors should choose to wait. Sensors update their neighbor information and decrease the random waiting time based on each "new" Hello message received.

This encourages those sensors with many neighbors to become cluster heads. If a neighbor declares itself to be a cluster head, the sensor cancels its own timer and joins the neighbor's new cluster. If the timer expires, then the sensor declares itself to be a cluster head, a focal point of a new cluster .By adjusting randomized waiting timers, the sensors can coordinate themselves into sensible clusters, which can then be used as a basis for further communication and data processing.

3.3 Gateway Selection

To interconnect two adjacent non-overlapping clusters, one cluster member from each cluster must become a gateway. According to the process of cluster formation, sensors can obtain local information and know the number of neighboring sensors in adjacent clusters. Therefore, given the local information, sensors may initialize their counters for gateway selection. Based on the counter, cluster heads broadcast messages to trigger the gateway selection process. After applying the procedure for determining gateways, the gateway nodes broadcast messages to update the connectivity information and activate the linked cluster architecture

3.4 Key Distribution and Renewal

The two symmetric shared keys, a cluster key and a gateway key, are encrypted by the pre-distributed key and are distributed locally. A cluster key is a key shared by a cluster head and all its cluster members, which is mainly used for securing locally broadcast messages, e.g., routing control information, or securing sensor messages. Moreover, in order to form a secure communication channel between the gateways of adjacent clusters, a symmetric shared key may be used to encrypt the sending message.

The challenge encrypted by a cluster key or a gateway key may be made to guard against anti-nodes. Therefore, the security of intra-cluster communication and inter-cluster communication are established upon a cluster key and a shared gateway key, respectively. Now the role of security key is handed over to cluster key and gateway key. After the cluster key and gateway key are created, the pre-distributed key can be ignored.

4.1 Key Renewal

Using the same encryption key for extended periods may incur a cryptanalysis risk. To protect the sensor network and prevent the adversary from getting the keys, key renewing may be necessary. Initially all cluster heads (CHs) choose an originator to start the "key renewals", and then it will send the index to all cluster heads in the network. After selecting the originator, it initializes the "Key renewal" process and sends the index to its neighboring clusters by gateways. Then the cluster head refreshes the two keys from the key pool and distributes the two new keys to their cluster members locally. The operation repeats the way through to all clusters in the network.

4. CONCUSION AND FUTURE WORK

In this paper concluded that the cross-layer design of energy efficiency secure scheme integrating the Medium Access Protocol there is no exact packet is involved in the original Medium Access Protocol design is scheme to reduce the authentication process to mitigate the power exhausting attack is used. The comparative analysis shows that the low power listening and elliptical curve cryptography protocol is used reduce the life time node and save the energy is performed.

REFERENCES

[1] M. Li, Z. Li, and A. V. Vasilakos, "A survey on topology controlling wireless sensor network the Taxonomy, comparative study, and open issues, "*Proc. IEEE*, vol. 101, no. 12, pp. 2538–2557, Dec. 2013.

[2] A. Bachir, M. Dohler, T. Watteyne, and K. K. Leung, "MAC essentials for wireless sensor the networks," IEEE Communication. Survey. Tuts., vol. 12, no. 2, pp. 222–248, Second Quarter 2010.

[3] J.Kabara and M. Calle, "MAC protocols used by wireless sensor networks and a general method of performance evaluation," Int. J. Distributed. Sensor Network., vol. 2012, pp. 1–11, 2012, Art.

[4] G. P. Halkes, T. van Dam, and K. G. Langendoen, "Comparing energy saving MAC protocols for wireless sensor networks," Mobile Network Appl., vol. 10, no. 5, pp. 783–791, 2005.

[5] Ye, J. Heidemann, and D. Estrin, "An energy-efficient MAC protocol for wireless sensor networks," in *Proc. 21st Annu. Joint Conf. IEEE Computer. Communication. Soc. (INFOCOM)*, Los Angeles, CA, USA, 2002, vol. 3, pp. 1567–1576

.

[6] T. van Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in Proc. 1st Int. Conf. Embedded Network Sensor Syst. (SenSys), Los Angeles, CA, USA, 2003, pp. 171–180.

[7] J. Polastre, J. Hill, and D. Culler, "Versatile low power media access for wireless sensor networks," in Proc. 2nd Int. Conf. Embedded Netw. Sensor Syst. (SenSys), Baltimore, MD, USA, 2004, pp. 95–107.

[8] M. Buettner, G. V. Yee, E. Anderson, and R. Han, "X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks," in Proc. 4th Int. Conf. Embedded Netw. Sensor Syst. (SenSys), Boulder, CO, USA, 2006, pp. 307–320.

[9] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols," IEEE Trans. Veh. Technol., vol. 58, no. 1, pp. 367–380, Jan. 2009.

[10] R. Falk and H.-J. Hof, "Fighting insomnia: A secure wake-up scheme for wireless sensor networks," in Proc. 3rd Int. Conf. Emerg. Security Inf., Syst. Technol. (SECURWARE), Athens, Greece, Jun. 2009, pp. 191–196

[11] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme for power exhausting attacks in wireless sensor networks," in Proc. 3rd Int. Conf. Ubiquitous Future Netw. (ICUFN), Dalian, China, Jun. 2011.

[12] C.-T. Hsueh, Y.-W. Li, C.-Y. Wen, and Y.-C. Ouyang, "Secure adaptive topology control for wireless ad-hoc sensor networks," Sensors, vol. 10, no. 2, pp. 1251–1278, 2010

.

[13] K.-T. Chu, C.-Y. Wen, Y.-C. Ouyang, and W. A. Sethares, "Adaptive distributed topology control for wireless ad-hoc sensor networks," in Proc. Int. Conf. Sensor Technol. Appl. (Sensor Communication), Valencia, Spain, 2007, pp. 378–386.

[14] A. Perrig, R. Szewczyk, J. D. Tygar, V.Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," Wireless Network., vol. 8, no. 5, pp. 521–534, 2002

[15] T. Dimitriou and I. Krontiris, "A localized, distributed protocol for secure information exchange in sensor networks," in Proc. 19th IEEE Int. Parallel Distributed. Process. Symp., Denver, CO, USA, Apr. 2005.