INTERNATIONAL JOURNAL OF REVIEW AND RESEARCH IN APPLIED SCIENCES AND ENGINEERING(IJRRASE)

ISSN: 2231-0061

Journal home page: www.ijcns.com email: gopalaxpapers@yahoo.com.sg

Volume : 7 Number : 1 Year :2015 Pages: 20-27

Distributed Key Management System For Secret Key Using Elliptical Curve Cryptography Scalar Multiplication Technique

---

A.VIJAY VASANTH
Senior Assistant Professor
Department of Computer science and Engineering
Christ College of Engineering & Technology
Pondicherry, India

M.SHANTHINI
M.Tech, Dept. of Computer science and Engineering
Christ College of Engineering & Technology
Pondicherry-605110, India
shanthini.flower@gmail.com

G.JEYALAKSHMY
M.Tech, Dept. of Computer science and Engineering
Christ College of Engineering & Technology
Pondicherry-605110, India
jeyalakshmy.gopal@gmail.com

D.SUGANYA
M.Tech, Dept. of Computer science and Engineering
Christ College of Engineering & Technology
Pondicherry-605110, India
suganyamtechcse@gmail.com

Article history:

Received 22-10- 2015
Accepted 10-11-2015

Reviewed by:
1.Dr. G.Ramesh
2.Dr. H.Charumathi

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

ABSTRACT: In Wireless Sensor network design the Security and the energy efficiency are different concern. The Low Power Listening protocol and Duty cycle protocol are used for energy conversation in wireless sensor network. The Energy Efficiency Secure adaptive topology control protocol algorithm used to form hierarchical topology against power exhausting to distribution the keys. 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 awake sensor node to awake node extend the life time of sensor node.

1. INTRODUCTION

Wireless Sensor Network is used collect data form environment. It consists of large number of sensor node and one or more base stations. The node in the network are 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. 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.

A Sensor network consists of multiple detection stations called sensor nodes. Each node is small, lightweight and portable.

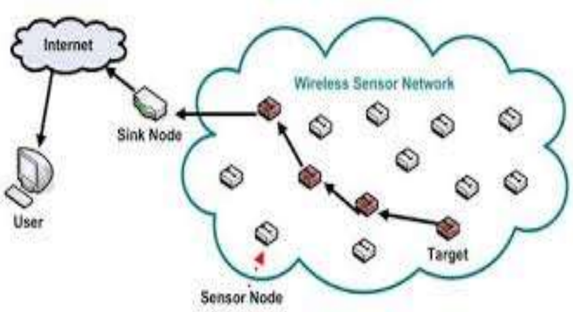

Fig. 1.1 Wireless Sensor Network

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. SECURE TOPOLOGY

The Secure adaptive topology control protocol algorithm is involved to form hierarchical topology in four phases:

PHASE - 1 ANTI – NODE DETECTION

The Network robust against attacks, an authenticated broadcasting mechanism, a plaintext “Hello” message is encrypted by the pre-distributed they as the broadcasting challenge. If the sensor network cannot decrypt the receiver message successfully, the sender is said to be anti-node detection in order to make safe network.

PHASE – 2 CLUSTER FORMATION

When Sensor are first deployed, the ADTCA from may be used to partition the sensor into cluster.

Cluster head Selection: Each sensor sets a random waiting timer, broadcast its presence via a “Hello.” The Sensor that hear many neighbors are good candidates for initiation new cluster; those with few neighbor should choose to wait. Sensor update their neighbor information and decrease the random waiting time based on each “new” Hello message received.

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, sensor can obtain local information and know the number of neighboring sensors in adjacent cluster. Therefore, given the local information, sensors may initialize their counters for gateway selection.

PHASE – 3 KEY DISTRIBUTION

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 mainly used for securing locally broadcast message. The security of intra-cluster communication and inter-cluster communication channel are established upon a cluster key and a shared gateway key.

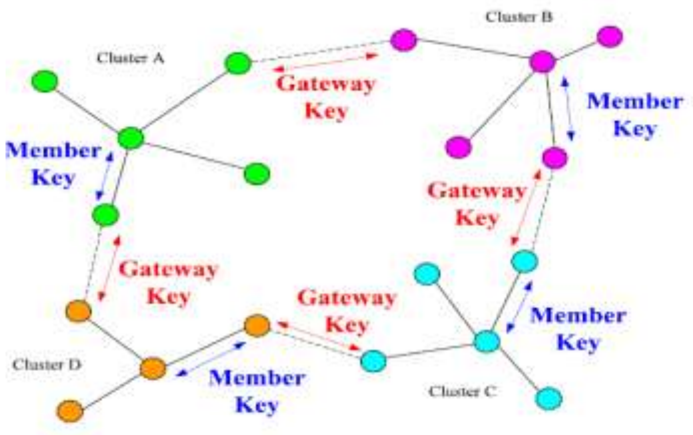

Fig 1.2 Key Distribution for WSNs

PHASE – 4 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 choose an originator to start the “key renewals”, and then it will send the index in the network. After selecting the originator, it initializes the “key renewal” process and sends the process. Then the cluster header refreshes the two keys from the key pool and distributed the two new keys to their cluster member locally.

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

3.1 Low Power Listening Protocol

A protocol transmit packets which allows the nodes to sleep for the long period of the time between the channel problems. 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/received. 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 send 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 schemes is used.

3.3 Elliptical Curve Cryptography using Scalar Multiplication

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 Lenstra 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.

4 MEDIUM ACCESS PROTOCOL

Medium Access Protocols used for conventional wireless sensor network the medium access protocol is used for wired environment can’t be used in wireless environment because collision occurring at the receiver is to be avoided. In the wired network the sender detects collision but the since signal strength is virtually the same throughout the wired medium, this does not pose any significant problem. However the wireless network the signal strength depreciates in inverse proportion to the square of the distance.

The Medium Access Protocol in Wireless Sensor Application are:

1) Low Power Operation

2) Effective Collision Avoidance
3) Simple Implementation, Small Code and RAM Size
4) Efficient Channel Utilization at Low and High Data Rates
5) Reconfigurable by Network Protocols
6) Tolerant to Changing RF/Networking Conditions
7) Scalable to Large Numbers of Nodes

The Medium Access Protocol has major categories:
1) Controlled Access Protocol
2) Random Access Protocol

1) Controlled Access Protocol

The Controlled Access Protocol nodes are allocated time slots are using TDMA or FDMA in the combination of the TDMA. In the given each time slot a node has access to the shared medium and can transmit without collision. The TDMA, nodes consists of the allocated the different times such that at time t2, node N3 has access to the medium. The Receiver nodes are synchronization with their sender nodes to wake up at the same time. This protocol enhances energy efficiency by avoiding collision and overhearing. However a lot of overhead is incurred in synchronization, which together with clock drift is an issue with this protocol.

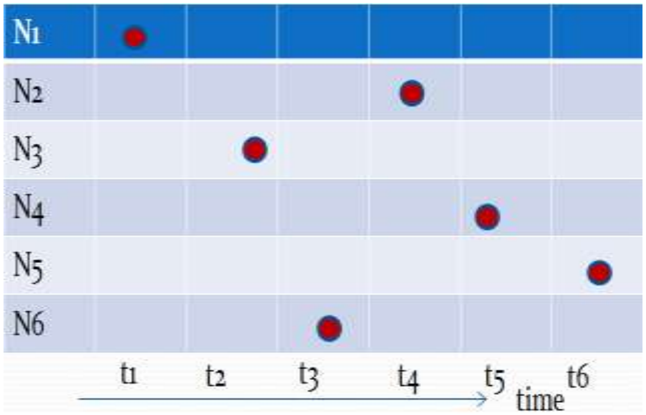

Fig. Controlled Access Protocol

2) Random Access Protocol

The Random Access Protocol are less compounded than the Controlled Access protocols and also they can be completely distributed thus endangering more Scalability. The CSMA/CA is used by the nodes to access the medium with no master-slave relationships but all the nodes competed to gain access to the channel. It is less processing and smaller memory are required in Random Access Protocol because of no need to schedule all the nodes thereby reducing control overhead which is the main source of energy drain in Controlled Access Protocol. Invariably, the rate of collision is higher and actually the main concern in Random Access Protocol. CSMA/CA, though has good scalability, consumes more power and offers low bandwidth utilization during heavy traffic. Also Random Access Protocol. These uses preamble sampling or low power listening which occupies the channel for longer time than data packets while hidden stations' preambles keep colliding.

It is concluded that, by combining other protocols such as controlled or the random access protocol with wireless sensor network , then the nodes can be reachable by all the wireless network nodes and this paper address the security concerns in wireless networks

5.ALGORITHM USED FOR THE COMMUNICATING NODE IN THE NETWORK

5.1 Shortest Path Algorithm

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. T-MAC uses less energy than S-MAC.

We expected this, because in the nodes-to-sink communication the load varies with the location of nodes: there is more in the neighborhood of the sink node. This also explains why the absolute load is much lower for or nodes-to-sink than for local unicast the rate at which the sink can handle incoming messages limits the load individual nodes can generate without congesting the network. As with homogeneous local unicast we see that the maximum throughput of T-MAC is less than that of S-MAC. Our experience with other message sizes and communication patterns is that the maximum throughput of T-MAC is at worst about 70% of S-MAC. We do not worry about too much about T-MAC's reduced maximum throughput, because it only occurs under extreme loads that are best avoided by sensor applications.

5.2 Event – Based Local Unicast and Node-to-Sink

The Event based local unicast and node-to sink with a complete scenario. When no events happen, nodes exchange local messages of 10 bytes with each other every 20 seconds. They also report to a sink node every 100 seconds. When an event happens nodes in the neighborhood of the event start sending local unicast messages of 30 bytes, with a rate of 4 per second.

They then also send messages of 50 bytes to the sink, the second. These are the messages are aggregated in the network which is able to handle a short-lived burst of S-MAC must choose a long active part of the duty cycle S-MAC therefore wastes much energy at times when no events happen. By the adaptively changing the duty cycle, T-MAC can decrease the used energy in this scenario.

The event based local the process towards a more realistic scenario. In this process, events occur in the network with a frequency of one per 10 seconds. Events have an average duration of 5 seconds and an area of approximately 9 nodes. These nodes then send local unicast messages to their neighbors for the duration of the event. A neighbor that receives one of these messages replies with a probability of 20%. We performed multiple measurements, with different message frequencies during events. This frequency is on the horizontal axis of the graph. For T-MAC, we used overhearing avoidance but no FRTS and no full buffer priority.

Especially when the message frequency during events increases. However, the maximum frequency that T-MAC can handle is lower than that of S-MAC, like the nodes-to-sink communication pattern. Again, T-MAC source from the early sleeping problem, because we have relatively many edge nodes.

The Collisions if two nodes transmit at the same time and interfere with each the others transmission, packets are corrupted. Hence, the energy used during transmission and reception is wasted. The protocol overhead most protocols require control packets to be exchanged there as these contain no application data, we may consider any energy used for transmitting and receiving these packets as overhead The overhearing since the air is a shared medium, a node may receive packets that are not destined for it; it could then as well have turned it’s the radio. The encryption of the

Function and decryption function is used for the clock cycle execution can be measures is performed.

Conclusion and future

In this paper, we concluded that the 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. ID 834784.

[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] W. 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.