ISSN No. 0976-5697

Volume 6, No. 5, May - June 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# Authentication and Hybrid Security in Heterogeneous Wireless Sensor Network

Majida Chettiyam Veettil
Computer Science & Engineering
KMCT College of Engineering
Kozhikode, Kerala

Sandhya V
Asst. Professor, CSE
KMCT College of Engineering
Kozhikode, Kerala

Niyas N
Asst. Professor, CSE
Kozhikode, Kerala
KMCT College of Engineering

***Abstract***: Security in communication network is the major threat in passing data among the nodes of a Wireless Sensor Network. Establishing an efficient key management in wireless sensor networks (WSN) and providing authentication to the nodes is a great challenge with reference to the constrained energy, memory, and computational capabilities of the sensor nodes. Previous researches on network security mainly considered homogeneous sensor networks with symmetric key cryptography. Recent researchers advanced to asymmetric key cryptography in heterogeneous sensor networks (HSN) that can improve network performance. The merits and demerits of symmetric and asymmetric cryptography were studied in combination with authentication methods, and thus proposing Authentication and Hybrid Security in Heterogeneous Wireless Sensor Networks .Tickets are used by the cluster heads to communicate to base stations, public key encryption method based on Elliptic Curve Cryptography (ECC) to communicate between H and L sensor nodes while using a hash function between adjacent nodes in the same cluster. The combined authenticated and key management method provides better security with minimum communication and computation cost based on analysis and simulation.

***Keywords***: symmetric key cryptography, asymmetric key cryptography, homogeneous sensor networks, heterogeneous sensor networks, authentication, hash function, ECC

## I.INTRODUCTION

Wireless Sensor Networks (WSNs) [1] consists of tiny devices called sensors, which are deployed to co-operatively process and communicate the data about a targeted environment. They have a wide range of application like military and national defense, medical care, environmental monitoring, wildlife tracking, weather checking applications, traffic management and many other areas [1].People can access a large number of detailed, reliable information at any time, place and environment. The sensor nodes deployed in a hostile environment can be used to detect, monitor and collect the data, and to perform decision making and evaluation. They can be eavesdropped, captured and compromised. Sensor nodes detect enemy intrusion in battle field, measure various environmental variables and keep the information secret for which it is important to establish a secure communication between the sensor nodes. For secure communication between two sensor nodes, a secret key is present. Hence, WSNs security serves to conserve the confidentiality, integrity and availability of the transmitted information.

Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning motes of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications band-width. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. Sensor networks are self organized networks, which makes them suitable for dangerous and harmful situations, but at the same time makes them easy targets for attack. For this reason we should apply some level of security so that it will be difficult to be attacked, especially when they are used in critical applications Sensor nodes are randomly deployed in special areas to collect information. Since the data packets are transmitted over the air, it is not difficult for the adversaries to steal information by eavesdropping. To guarantee the confidentiality of information transmitted between sensor nodes, the messages should be encrypted before being transmitted. It is a great challenge to implement encryption algorithms in wireless sensor networks because of the constrained resource. Furthermore, malicious nodes may impersonate to be legitimate nodes and communicate with other valid nodes. This may subvert the whole networks. Generally, all sensor nodes in a WSN may be divided into several small groups which are known as clusters .Each cluster would have a cluster head responsible for collecting and aggregating sensing data from its cluster members. A cluster- based WSN can be implemented in both homogeneous WSN and heterogeneous WSN.

Providing security is a complicated task compared to a traditional wired network or a mobile ad- hoc network due to many reasons like nodes resource constraints, the wireless communication employed, deployment methods, location of the field of interest and presence of huge number of nodes in the network. These sensor nodes have low processing power, less memory capacity and less battery life. [2] Due to these limitations, WSNs have been divided into homogeneous WSN and heterogeneous WSN. All sensor nodes in homogeneous WSN have the same capabilities and heterogeneous WSN incorporate different types of sensor nodes with different capabilities. They contain a small number of powerful high-end H sensor nodes and a large number of low-end L sensor nodes [3]. Key management can be defined as can be mainly classified into two categories: Static and dynamic key management schemes. All keys are pre-distributed in sensor nodes in the static key management schemes. These schemes are based on the probabilistic key redistribution that guarantees a high probability of sharing keys between nodes [4] In the dynamic key management scheme, some keys or key seeds are predistributed in sensor nodes and the session keys are established on demand. Mostly there are some nodes acting as group heads or gateways and these intermediate nodes are usually more powerful than other member nodes in terms of energy supply, transmission range, data processing capability, storage capacity, and tamper resistance [5].

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. Kerberos relies exclusively on conventional encryption, making no use of public-key encryption

The paper proposes an efficient, authenticated and hybrid wireless sensor network. Considering the difference of the capacities of sensor[6] and the advantages and disadvantages of symmetric key cryptography and asymmetric key cryptography, in a layered network model, communication to the base station is highly secured with the usage of a third party authentication protocol called Kerberos and usage of lightweight public key encryption method called Diffie Hellman based on elliptic curve cryptography (ECC)[7]to communicate between H and L nodes, while using symmetric key encryption method based on a one-way hash function between adjacent nodes belong to the same cluster. The analysis and simulation results show that the proposed key management method can provide better security and scalability.

## II.RELATED WORK

WSNs have been divided into homogeneous WSN and heterogeneous WSN. All sensor nodes in homogeneous WSN have the same capabilities and heterogeneous WSN incorporate different types of sensor nodes with different capabilities. They contain a small number of powerful high-end sensor nodes (H sensors) and a large number of low-end sensor nodes (L sensors) .Key management deals with the secure generation, distribution, and storage of keys. Secure method of key management is extremely important and can be mainly classified into two categories: static and dynamic key management schemes. All keys are pre-distributed in sensor nodes in the static key management schemes. These schemes are based on the probabilistic key redistribution that guarantees a high probability of sharing keys between nodes [6]. In the dynamic key management scheme, some keys or key seeds are predistributed in sensor nodes and the session keys are established on demand. Mostly there are some nodes acting as group heads or gateways and these intermediate nodes are usually more powerful than other member nodes in terms of energy supply, transmission range, data processing capability, storage capacity, and tamper resistance.

Eschenauer et.al [10] proposes a probabilistic key redistribution technique called basic scheme or E-G method. Basic scheme picks a random set of keys S out of the total possible key space. The nodes first perform key-discovery to find out the neighbors sharing the same key. This shared key then becomes the key for that link. After key-setup is complete, a connected graph of secure links is formed. Nodes can then set up path keys with nodes in their vicinity that did not share keys within their key rings. If the graph is connected, a path can be found from a source node to its neighbor. The source node can then generate a path key. The method relies on probabilistic key sharing among the nodes of a random graph and also uses simple protocols for shared-key discovery and path-key establishment, and for key revocation. But this method holds some disadvantages like high key-sharing probability is required and random selection of key ring from a key pool. Even large number of keys is preloaded in each sensor in order to achieve high key-sharing probability and for key pre distribution large storage space should be provided.

Haowen Chan et. al [11] investigated the random-pair wise keys scheme, which assures that, even when some numbers of nodes have been compromised, the remainder of the network remains fully secure. Furthermore, this scheme enables node-to-node mutual authentication between neighbors and quorum-based node revocation without involving a base station. Node-to-node mutual authentication here refers to the property that any node can ascertain the identity of the nodes that it is communicating with. The q-composite keys scheme operates similar to that of the basic scheme, differing only in the size of the key pool S and the fact that multiple keys are used to establish communications instead of just one.

Reza Azarderakhsh et. [12] al proposed a key management method based on ECC. Cluster heads send session key of adjacent nodes with ECC. Since the session keys of adjacent nodes are different, the security of communication between other nodes when a node is captured will not be threatened.

It provides a good resilience. But each ordinary node need store public keys of all cluster heads, which increases the storage consumption. The key management method used here makes use of both private and public key cryptography. Public key cryptography is used to establish a secure link between sensor nodes and gateways. Instead of preloading a large number of keys into the sensor nodes, each node requests a session key from the gateway to establish a secure link with its neighbors after clustering phase.

Du et al. [14] proposed routing-driven elliptic curve cryptography where a node just needs to establish communication with a small portion of its neighbors called c-neighbors and does not need to setup shared keys for each pair of neighbor sensors. According to the routing information, cluster heads encrypt session keys with ECC and then sent them to adjacent nodes which need to establish communication .This method significantly reduce the overhead of key establishment, communication and computation overheads, and hence reduce sensor energy consumption. The recent implementation of shows that an ECC point multiplication takes less than one second, which demonstrates that the ECC public-key cryptography is feasible

for sensor networks. Compared with symmetric key cryptography, public-key cryptography provides a more flexible and simple interface, requiring no key pre-distribution, no pair-wise key sharing, and no complicated one-way keychain scheme.

## III.PROPOSED MODEL

Secret communication is an important requirement in many sensor network applications, so shared secret keys are used between communicating nodes to encrypt data. Some of the major constraints like ad hoc nature, intermittent connectivity, and resource limitations of the sensor networks prevent traditional key management and distribution schemes to be applicable to WSN. It is not possible to setup an infrastructure to manage keys used for encryption in the traditional internet style because of factors such as unknown and dynamic topology of such networks, vagaries of the wireless link used for communications, and lack of physical protection. A practical solution given these constraints is to pre-load the keys on the sensors before the sensor nodes are deployed. Then use the maximum known methods to make it safe to pass the message through the network without intruders trying to eavesdrop. Or if so, hide the contents as much as possible by which ever means.

One such solution [fig 1] is to provide authentication to the user or system and then use encryption for better safety. Here the combination of Kerberos authentication along with symmetric and asymmetric encryption makes it hybrid and efficient. Initially all nodes are assumed to be stationary and the public and private keys of all nodes will be loaded in the base station. The base station itself is a node with maximum energy. Each cluster will select one node with higher energy as their head and forms the cluster head. The communication is through the cluster head only to the base station and from base station to L nodes. The low energied L sensors are not tamper resistant while the high energied H sensors are tamper resistant.

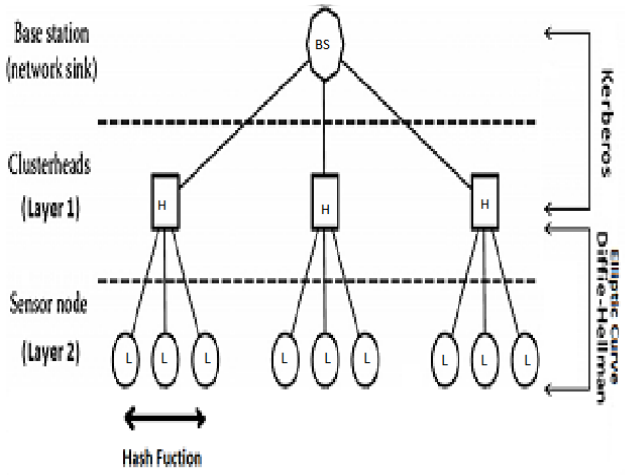
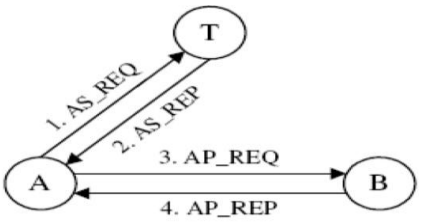



Fig:1 Structure of Proposed System

Kerberos [8] provides an authentication method with which the cluster head communicates with base station and for the base station to pass the message to the cluster heads of other cluster. Nodes register only once and are trusted in the complete network for the rest of the session. To have a secure network, the following requirements must be met:
(i)Have all users prove their identity for each desired service and make sure that no one can take the identity of someone else.(ii)Make sure that each network server also proves its identity.
Otherwise an attacker might be able to impersonate the server and obtain sensitive information transmitted to the server. This concept is called mutual authentication, because the client authenticates to the server and vice versa. Kerberos helps you meet these requirements by providing a strongly encrypted authentication. Two versions of Kerberos are available: Kerberos Version4 and Kerberos Version5.
Here the light weight version of Kerberos [18] [fig 2] is used.




1. AS_REQ: $A, B, n_A$
2. AS_REP: $\{ k_{AB}, B, t_S, t_E, n_A \} k_{AT}$ , $\{ k_{AB}, A, t_S, t_E \} k_{BT}$
3. AP_REQ: $\{ k_{AB}, A, t_S, t_E \} k_{BT}$ , $\{ A, t_A \} k_{AB}$
4. AP_REP: $\{ t_A \} k_{AB}$

Fig:2 Light Weight Kerberos Authentication

The ticket obtained is used by the cluster head to communicate data to the base station. And the base station also uses this ticket to pass the message to the next cluster head. Here the base station is assumed as a node which has maximum energy.
Diffie Hellman key exchange (DH) [9] is a specific method of securely exchanging cryptographic keys over a public channel and was the first specific example of public-key cryptography as originally conceptualized by Ralph Merkle. The Diffie Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communication channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher Elliptic Curve Cryptography [9] is the current standard for public key cryptography, and is being promoted by the National Security Agency as the best way to secure.

Diffie-Hellman (ECDH) key exchange algorithm based on ECC can be used to establish shared key between the cluster head and nodes in its cluster. Suppose that *Hj* and *Li* need to establish a shared key [1].

*Hj* generates the shared key:

$$K_{HjLi} = P^r_{H_j} \cdot P^u L_i = P^r_{Hj} \cdot P^r_{Hj} \cdot G$$

$L_i$ generates the shared key:

$$K_{LiHj} = P^r_{Li} \cdot P^u_{Hj} = P^r_{Li} \cdot P^r_{Hj} \cdot G$$

*G* is a base point of the elliptic curve.Now both the H and L sensor share a common key and using this they communicate with each other.

The leaf nodes, that is, L sensor nodes, due to the limited energy cannot use public key encryption and henceforth make use of the hash function to generate symmetric session keys. This can be done when H sensor generate a random number r which can be encrypted with the previously generated shared key $K_{HL.}$ If u and v are the neighboring L sensor nodes then,

$$K_{uv}=\text{hash}\ (r\backslash\backslash id_u\backslash\backslash id_v)$$

And using this key they can communicate.

At a time the L sensor can use hash function to communicate to peer nodes or use the ECDH to pass the message to the H sensor and the H sensor can use this same key to pass message back to L of same group else the cluster head will make use of the ticket obtained from the base station to communicate and finally the base station use only the ticket to communicate to cluster heads.

## IV.PERFORMANCE

The evaluation of the energy cost of cryptographic key establishment was conducted on a WINS sensor node [21] and [20].The energy characteristics of the WINS node reported in [22] were used for energy calculation which is the product of average power consumption and the execution time. The communication energy depends on the distance between sending and receiving node and the time required for sending the message, which it is proportional to the message length and to the transmission rate. Also, the transmission of messages consumes energy on the sending and the receiving node. For the graph generation purpose simulation study was done and obtained the energy consumption versus no. of cycles of data transmitted for

Cluster heads, L sensors and Base Station [fig 3]

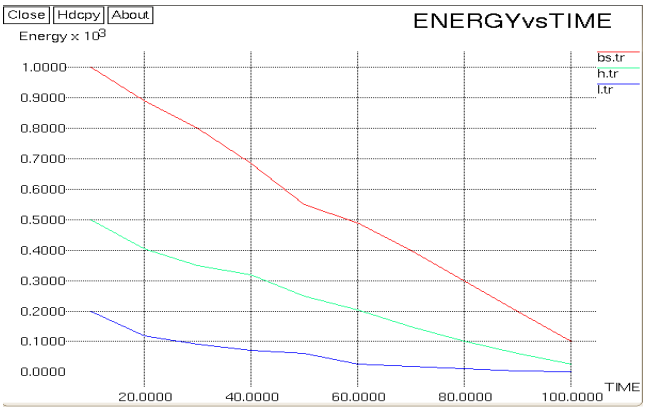
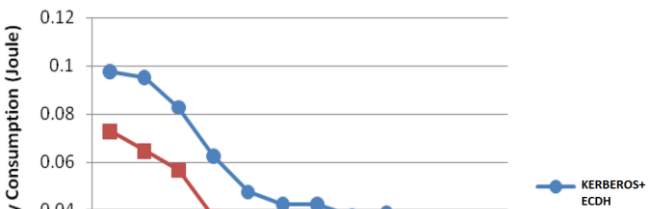



Fig: 3 Energy consumption in Base Station,Cluster Head and L sensor

It is found that in Cluster head and Base Station there is a gradual decrement of energy as the time increases. The performance of a normal node has a sudden fall in the graph, showing the degradation of energy among the L sensors. The graph analysis finds that the energy among the nodes decreases after time. There is only a slight variation in the graphs except that among L sensors there is a faster reduction in energy compared to Cluster head and Base Station. The Base Station with the maximum energy,




The system was compared with the [1] and with reference to the work done in [19] and [20], it has been verified that Kerberos-ECDH is around one order of magnitude less costly than the ECDSA-ECDH key exchange [fig 4]. It should be performed only when a trusted third party is available.

## V.CONCLUSION AND FUTURE SCOPE

The project utilizes a network authentication protocol developed as a solution to network security problems like sniffing, eavesdropping etc. It is a highly secure protocol for preventing attacks and thus increasing security of WSN. It is mainly applicable for critical areas like defence, military etc. were data are needed to be kept highly confidential. It produces a system with lesser communication and computation cost. Practical experiments were conducted on TelosB motes and MicaZ sensors and proved that the comparative computational and communicational energy consumption is lower than earlier methods like ECDSA. The PKE method utilized doesn't reveal the key as it doesn't send the key in its original form. Kerberos authentication is one step lesser in energy consumption compared to that of other authentication methods like ECDSA. Combined usage of both symmetric and asymmetric cryptography provides hybrid security.ECDH can be replaced with ECMQV (Meneze-Qu-Vanstone) which is a key agreement protocol with implicit authentication as a future scope.

## VI. REFERENCES

[1] Zhang Ying, JiPengfei, "An efficient and Hybrid Key Management for Heterogeneous Wireless Sensor Networks", 26th Chinese Control and Decision Conference (CCDC) IEEE, 1881-1885, 2014.

[2] K. Romer, F. Mattern, \The design space of wireless sensor networks, Wireless Communication", IEEE 11 (2004) 5461.

[3] A.K. Das, \An unconditionally secure key management scheme for large-scale heterogeneous wireless sensor networks\, in: Proceedings of the First International Conference on Communication Systems and networks, IEEE Press, Bangalore, India, 2009, pp. 653662.

[4] M. Boujelben, H. Youssef, R. Mzid, M. Abid, "IKM an identity based key management scheme for heterogeneous sensor networks\, Journal on Communications 6 (2) (2011) 185197

[5] X. Du, Y. Xiao, and Guizani. An effective key management scheme for heterogeneous sensor networks. Ad Hoc Networks, 5(1):2434, 2007.

[6] Gupta P, Kumar P R. "The capacity of wireless networks"[J]. IEEE Transactions on Information Theory, Vol.46, No.2,388-404, 2000

[7] Atul Kahate "cryptography and Security\, Volume2

[8] William Stallings "Cryptography and Network Security\, Fourth Edition

[9] Koblitz N. Elliptic curve cryptosystems. Mathematics of computation, Vol.48, No.177, 203-209, 1987

[10] Eschenauer L, Gligor V D. "A key-management scheme for distributed sensor net-works\//Proceedings of the 9th ACM conference on Computer and communications security ACM", 41-47, 2002

[11] Chan H, Perrig A, Song D. \Random key predistribution schemes for sensor networks\, 2003'Symposium on Security and Privacy. IEEE, pp. 197-213, 2003.

[12] Azarderakhsh R, Reyhani-Masoleh A, Abid Z E. "A key management scheme for cluster based wireless sensor networks", EUC'08. IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. IEEE, Vol.2, 222-227, 2008

[13] Du X, Guizani M, Xiao Y, et al. \Transactions papers a routing-driven Elliptic Curve Cryptography based key management scheme for Heterogeneous Sensor Networks".' Wireless Communications, IEEE Transactions on, Vol.8, No.3, 1223-1229, 2009.

[14]Zhou R, Yang H. \A hybrid key management scheme for Heterogeneous wireless sensor networks based on ECC and trivariate symmetric polynomial\, 2011 International Conference on Uncertainty Reasoning and Knowledge Engineering (URKE)`. IEEE, Vol.1, 251-255, 2011

[15] Zhang Ying, JiPengfei, "An Efficient and Hybrid Key Management for Heterogeneous Wireless Sensor Networks", 26th Chinese Control and Decision Conference (CCDC) IEEE, 1881-1885, 2014.

[16] Karp B, Kung H T. GPSR: Greedy perimeter stateless routing for wireless networks, Proceedings of the 6th annual international conference on Mobile computing and networking.ACM, pp. 243-254, 2000.

[17] Qasim Siddique, \Kerberos Authentication in Wireless Sensor Networks\, Annals. Computer Science Series. 8th Tome 1st Fasc, 2010.

[18] N.S. Fayed *, E.M. Daydamoni, A. Atwan,"Efficient combined security system for wireless sensor network "Egyptian Informatics Journal (2012) 13, 185190

[19] Giacomo de Meulenaer, Francois Gosset, Francois-Xavier ,Standaert Luc Vandendorpe,\On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks", UCL/DICE Crypto Group

[20] Johann Grosch adl, Alexander Szekely, Stefan Tillich, \The Energy Cost of Cryptographic Key Establishment in Wireless Sensor Networks", Institute for Applied Information Processing and Communications

[21]Agre J, Clare L, Pottie G, Romanov N. Development platform for self-organizing wireless sensor networks. In: Unattended ground sensor technologies and applications of Proceedings of SPIE, vol. 3713. SPIE; 1999. p. 257–68.

[22] V. Raghunathan, C. Schurgers, S. Park, M. Srivastava"Energy-aware wireless micro sensor networks" IEEE Signal Process Mag, 19 (2) (2002), pp. 40–50