Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 10; April-June, 2015 pp. 61-68
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

Analysis of Secure Communication in Wireless Sensor Networks

Pratik P. Bheley[1] **and Voore Subba Rao**[2]

[1]Dept. of Electronics Engineering, RGCER, Nagpur
[2]Systems Admin Dept. Adcc Info CAD Ltd., IT Park, Near VNIT, Nagpur.
E-mail: [1]pratik24bheley@yahoo.com, [2]vsrao.voore@rediffmail.com

Abstract—*A Wireless Sensor Networks (WSN) of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. Kerberos authentication architecture for clusters in sensor network and to save energy of the sensor nodes and also to save time for data communication between the sensor nodes. The idea of having different Kerberos authentication architecture for the different clusters in sensor network. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. With the enhancement model of the Kerberos this paper also give importance to a combined system that use the two protocols, Lightweight Kerberos protocol and Elliptic Curve Menezes-Qu-Vanstone(ECMQV) protocol to enhance the security of the network and improve the energy consumption in the network. Beside that it increases the network speed due to minimizing the number of communications and calculations.*

Keywords*: Wireless Sensor Networks, Kerberos authentication architecture Lightweight Kerberos protocol*, *Elliptic Curve Menezes-Qu-Vanstone(ECMQV) protocol*.

1. INTRODUCTION

Recent advances in sensor technology (in terms of size, power consumption, wireless communication and manufacturing costs) have enabled the prospect of deploying large quantities of sensor nodes to form Wireless Sensor Networks (WSN).. A Wireless Censor Network is generally a complex and most important is its components are less resourceful, and the components are more susceptible to failures A WCN comprises a set of nodes each of which is capable of transmitting to or receiving from other nodes The nodes in the network, among others, can be a computer, concentrator, end user terminal, mobile station, repeater acting as a transmitter/receiver, or a sensor node. Two nodes in a WCN, in contrast to a wired CN, are connected by wireless communication links either directly. The authentication of base station in the wireless sensor network based on the Kerberos server authentication scheme. [5].The communication between the other nodes with the help of wired or wireless communication. The node mobility in WCN makes network links have higher unavailability rates and makes the performance analysis of a WCN even more difficult .Fig. ure 1 and Fig. ure 2 depicts the communication and sensor node architecture in wireless sensor network. Earlier, the sensor networks consist of many small number of sensor nodes that were wired to a central processing station. Nowadays, the major focus is on wireless Sensing nodes. The design of wireless sensor networks requires consideration for several disciplines such as distributed signal processing, communications and cross-layer design. Wireless Sensor Networks: Signal Processing and Communications focuses on the theoretical aspects of wireless

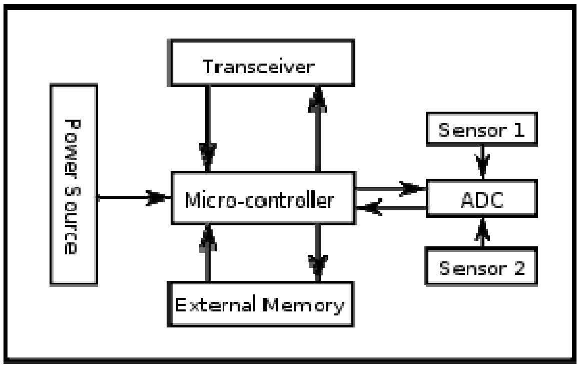


Fig. 1: Sensor node architecture

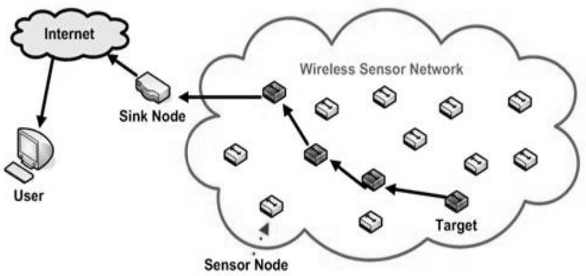


Fig. 2: Communication in WSN

sensor networks and offers readers signal processing and communication perspectives on the design of large-scale networks.

Because of the character of wireless communications, resource constraint on sensor nodes, size and density of the networks, and high danger of physical attacks to unattended sensors, it is a very important to provide security in WSNs. The main security requirement is to provide confidentiality, integrity, authenticity, and availability of all messages in the presence of resourceful adversaries. To provide secure communications for the WSNs, all messages have to be authenticated [4]. Modification of information is possible because of the nature of the wireless channels and uncontrolled node environments. In unsecure observations in WSN the opponent can modify information and also render the information unavailable. For that in WSN the importance is to provide security requirements.

2. RELATED WORK

Wireless Sensor Networks are composed of small, low cost, resource-constrained computing nodes equipped with low power wireless transceivers. Kerberos authentication scheme [4] is used for the authentication of base station in sensor network. It provides a centralized authentication server whose work is to authenticate user by providing to grant request to the base station.

2.1 Local communication

Neighboring nodes send localized messages to discover and coordinate with each other. A node may broadcast messages intended to be received by all neighboring nodes or unicast messages intended for a only single neighbor intended for only single neighbor.

In wireless sensor network a base station can't be trusted to identify its users correctly to network services. In particular the following three threads exist.

- The user access to a particular base station and pretend to be another user operating from the base station.
- The user exchange and use a reply attack to gain entrance to a base station or to interrupt operation.
- The user may alter the network address of a base station so that the request sent from the altered base station to come from the impersonated workstation.

Unauthorized user may gain access to the base station and collect the data that he or she is not authorized to access. Or otherwise conFig. uring provide in elaborates authentication protocol at each sensor node. Kerberos provide a centralized authentication server whose function is to authenticate users to servers and servers to users.

2.2 Tread to Networks

In an unprotected network environment, any client can apply to any server for service. It causes security risk is that of impersonation. An opponent can pretend to be another client and obtain unauthorized privileges on server machine. For this type of threat, servers must be able to confirm the identities of clients who request services.

Verification of the user in the wireless sensor network we have added the authentication scheme layer above the wireless sensor network which authorized the user to access the wireless sensor network without verification the user can't access the wireless sensor network. The authentication scheme is based on the Kerberos server authentication scheme. Kerberos is an authentication service, to give secure communication in Wireless Sensor Networks.

2.3 Traffic in Wireless Sensor Network

Traffic in sensor networks can be classified into one of three categories:

1). Many-to-one
Multiple sensor nodes send sensor readings to a base station or aggregation point in the network.
2). One-to-many
A single node (typically a base station) multicasts or floods a query or control information to several sensor nodes.

3.1 Kerberos Server Architecture

There are two main components of Kerberos servers

• Authentication Server
• Ticket Granting Server

1). Authentication Server
Authentication server knows the password of all the users and stores these in a centralized database. The authentication server shares a unique secret key with each server. These keys have been distributed to the user in some secure manners.

2). Ticket Granting Server
Ticket granting server issues tickets to users who have been authenticated to authentication server. Then the user first requests a ticket from the authentication server. This ticket is saved by the user. Each time the user authenticate itself the ticket granting server then grants a ticket for the particular server/Base Station.

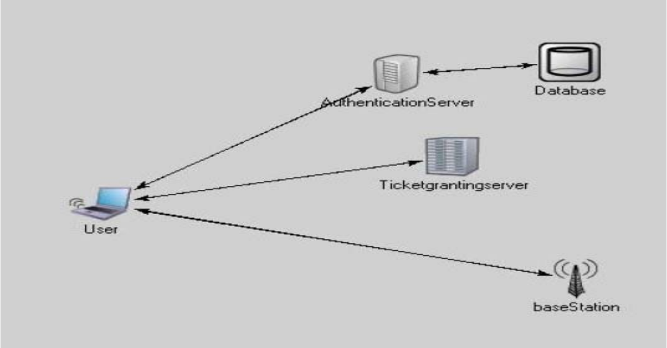


Fig. 3: A view of Kerberos

The user save each service granting ticket and uses it to authenticate its user to a server each time a particular service is requested.

E. Issuing Tickets for Authenticated Users

The Ticket granting server performs the work of issuing tickets to users who have been authenticated to authentication server. The first work that is to be performed is that the user first requests a ticket from the authentication server, and then this ticket is saved by the user. Each time the user authenticate itself, the ticket granting server grants a ticket for the particular server/Base Station. The user save each of the service granting ticket and uses it to authenticate to a server whenever a particular service is requested.

F. Loopholes in earlier proposed research work

Client requests a ticket granting ticket on behalf of the user by sending its users ID to the authentication Server.

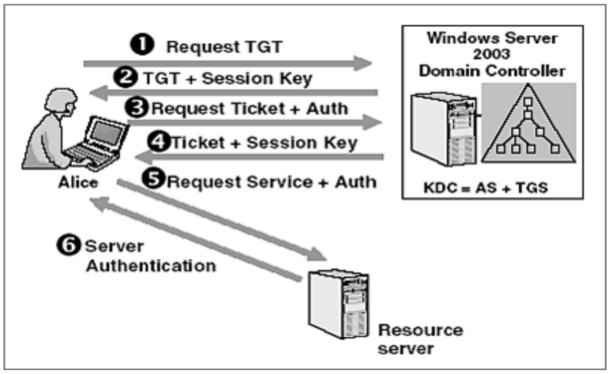


Fig. 4: The authentication service by Kerberos

- The authentication server responds with a ticket that is encrypted with a key. When the ticket arrives at the client, the client prompts the user for the password, generate the required and decrypt the incoming message.
- The client requests the service-granting ticket on behalf of the user. Then client transmit a message to the Ticket granting ticket containing the users ID and the ID of the desired service, and the ticket granting ticket.
- The ticket granting server verifies the ticket it checks that the time limit has not expired. Then the ticket granting ticket issues a ticket to grant access to the requested service.
- The client requests access to a service on behalf of the user. For this purpose the client transmits a message to the server containing the user ID and the service granting ticket. The server authenticates by using the contents of the tickets.

The major loopholes in earlier sensor networks were that each node in a wireless sensor network had only a single authentication centre i.e. the Kerberos.

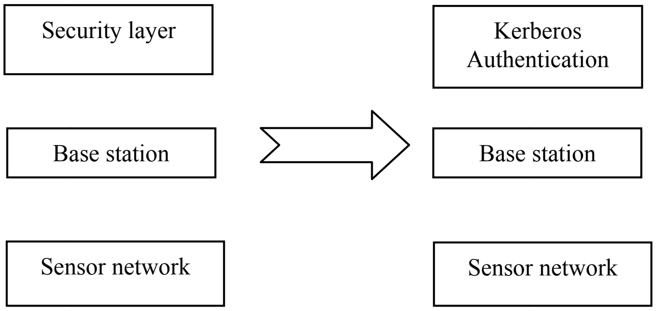


Fig. 5: Adding a new layer in Wireless Sensor Network

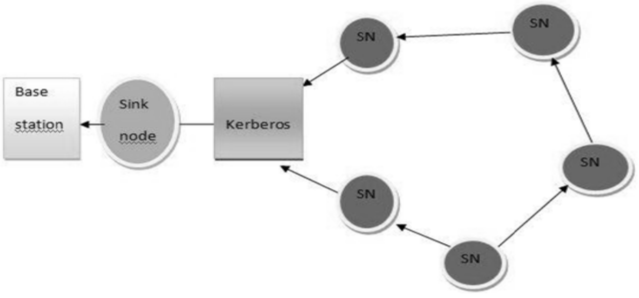


Fig. 6: Sensor network with a single Kerberos

Due to this, all the sensor nodes had to wait for a long time for their authentication and to establish connection with the sink node and the base station. The major disadvantage of this technique of communication was that each node suffered from energy loss with the wastage of time. There was a need to overcome this problem and check the efficient solutions for it.

3. PROPOSED TECHNIQUE

This paper proposes a solution for the above mentioned problem. Instead of serving one node at a time with the same Kerberos, clusters of sensor nodes in a wireless sensor network can be formed, each having its own authentication centre i.e. the Kerberos. This proposed solution will serve each node in the wireless sensor network by authenticating it through the particular Kerberos of that cluster and then letting the nodes to communicate with the sink node and finally the base station.

Lightweight Kerberos protocol with short messages [12] can be described as "Basic Kerberos authentication protocol without ticket granting service." To illustrate the idea of Lightweight Kerberos in authenticate two entities (Say A and B) to each other, Fig. 1 illustrates the message transfers between entity A and B and the trusted third party T (authentication server). Assume that A wishes to establish a session key with entity B and Both A and B share a long-term secret key with T. The description of the communication messages is as the following:

The first message is the Authentication Server Request (AS_REQ) message, which is sent from A to T. This message contains A’s identity, B’s identity, and a random nonce nA that will be used to associate reply messages with the matching AS_REQ request and to detect replays.

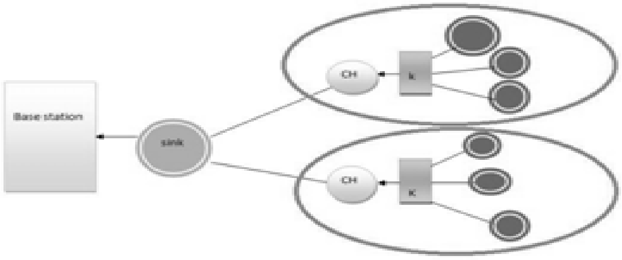
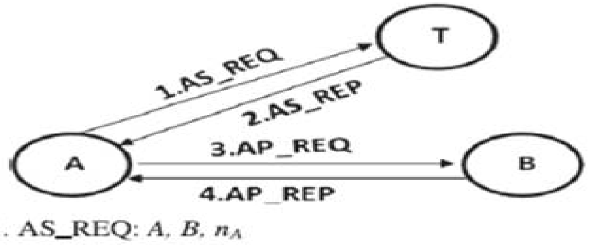


Fig. 7: Clusters of sensor nodes each with a Kerberos

More than one clusters of sensor nodes having their own authentication centre i.e. Kerberos. Each node of a cluster communicates with the authentication centre provided in the concerned cluster and then contacts to the sink node and further to the base station. This proposal will save the power of the sensor nodes and will make the communicating network efficient and reliable.

3.1 Advantage Of Proposed Technique with effective protocols

This technique can avoid more time and heavy traffic load with less energy consumption. In traditional network when more than one node send request to the Kerberos it takes more time to response which results in processing delay and leads to loss in energy of sensor nodes in sensor network. as will save the energy of the processing nodes. Hence it will be energy efficient technique. With the enhancement model of the Kerberos this paper also give importance a combined system that use the two protocols, Lightweight Kerberos protocol and Elliptic Curve Menezes-Qu-Vanstone(ECMQV) protocol to enhance the security of the network and improve the energy consumption in the network. Beside that it increases the network speed due to minimizing the number of communications and calculations.



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. 8: Simplified Kerberos protocol exchange (an expression of the form {X} k means that message X is encrypted using the keyk) [6].

1. Lightweight Kerberos protocol with short messages

Kerberos is a distributed authentication service that allows a client to prove its identity to a server without sending data across the network that might allow an attacker to subsequently impersonate the client. The basic Kerberos authentication protocol allows a client with knowledge of the user’s password to obtain a ticket and session key to prove its identity to any sever registered with the authentication server [18].

Lightweight Kerberos protocol with short messages [12] can be described as ‘‘Basic Kerberos authentication protocol without ticket granting service.’’ To illustrate the idea of Lightweight Kerberos in authenticate two entities (Say A and B) to each other, Fig. 8 illustrates the message transfers between entity A and B and the trusted third party T (authentication server). Assume that A wishes to establish a session key with entity B and Both A and B share a long-term secret key with T. The description of the communication messages is as the following:

- The first message is the Authentication Server Request (AS_REQ) message, which is sent from A to T. This message contains A’s identity, B’s identity, and a random nonce nA that will be used to associate reply messages with the matching AS_REQ request and to detect replays After receipt of the AS_REQ message, T looks up entities A and B in its database, verifies that they are authorized to establish a session key, and fetches their long-term keys kAT and kBT. Then, T generates a new random session key kAB to be shared between A and B and embeds it into a ticket. The ticket also contains A’s identity, and the ticket’s validity lifetime (expiration time tE and an optional starting time tS). The ticket is encrypted using kBT that only known by T and B. Next, T creates the AS_REP message, consisting of the ticket for A to present to B, kAB, tE, B’s identity, and nA from the AS_REQ message. All elements except the ticket are encrypted with kAT.
- After receiving of the AS_REP response, A uses kAT to decrypt the non-ticket part of the message. Entity A verifies that the received nonce matches the nonce it supplied in the AS_REQ message and that the current time is within the lifetime of the session key. In the third message, the AP_REQ (Application Request) message, entity A transfers the ticket together with an authenticator to B. The purpose of the authenticator is to prove that entity A knows kAB and to ensure that every AP_REQ message is unique.
- After receiving of the AP_REQ message, B decrypts the ticket using kBT and extracts kAB, the identity of A, and tE. Then, B uses kAB to decrypt the authenticator and compares the information in the ticket with that in the authenticator.

- If all checks pass, B considers A as authenticated. Mutual authentication requires that entity B proves its identity too by sending Application Reply (AP_REP) message, consists of the timestamp encrypted in the session key kAB, back to A. After A received and decrypted the AP_REP message, A verifies that the timestamp is the same one it sent in the AP_REQ message. This ensures A that kAB successfully transmitted to B.

Most of protocols uses third parity, like Kerberos, are three-way communication since two entities wishing to set up a secret key do not only transmit messages to each other but also to the trusted authority. Thus, the communication energy cost of Kerberos-like protocols is much higher than the energy required for calculating cryptographic primitives [20].

2. Elliptic Curve Menezes-Qu-Vanstone (ECMQV)

Elliptic Curve Menezes-Qu-Vanstone (ECMQV) is a key agreement performed using elliptical curves rather than traditional integers. The protocol was introduced by Laurie Law, Alfred Menenzes and others in “An Efficient Protocol for Authenticated Key Agreement”. ECMQV is authenticated, so it does not suffer Man in the Middle (MitM) attacks.

ECMQV protocol is based on Diffie–Hellman key agreement and modified to work in an arbitrary finite group and, in particular, elliptic curve groups. It is an example of key exchange protocols with implicit authentication [14].

In the ECMQV protocol each entity has both a static (i.e. long-term) public/private key pair and an ephemeral (i.e. short-term) key pair. A shared secret is derived using the static keys and the ephemeral keys, which guarantees that each protocol run between two entities A and B produces a different shared secret. Formally, an elliptic curve over a prime field GF(p) can be defined by a Weierstraß Eq. (1), where $\alpha, \beta \in GF(p)$ and $4\alpha 3 + 27\beta 2 \neq 0 \bmod p$ [21].

$$y2=x3+\alpha x+\beta$$

In what follows, let E be an elliptic curve group of order n, and G shall be a point on the curve. Assume that the order n is prime, which means that E is cyclic and G is a generator of E. Also, assume the domain parameters p, α, β, n, and G are publicly known to every entity of the network. Let A and B be two entities wishing to establish a shared key. First, entity A chooses a random secret number a with $2 \leqq a \leqq n - 2$, calculates $S = a \bullet G$. Entity B also chooses a random secret number b in the range of $[2, n - 2]$, calculates $T = b \bullet G$.

Entity A has the static key pair (a, S) which consists of a secret part (a) and a public part (S). Entity B has the static key pair (b, T) consisting of the secret key b and the public key T = b Æ G. The entities first exchange the public part of their static keys. After that, entity A and B perform the following steps to agree on a shared secret: First, entity A generates the ephemeral key pair (c, U), whereby U= c Æ G, and entity B generates the ephemeral key pair (d, V) with V =d Æ G. They exchange the public parts of these ephemeral keys. After that, entity A knows its own secret keys a, c, and the public keys S, T, U, and V. Also, B knows b, d, S, T, U, and V. The shared secret K is determined by entity A as in Algorithm 1. B also compute the same value of K by swapping (a, c, T, U, V) in Algorithm 1with (b, d, S, V, U) [22].

Algorithm 1: ECMQV key derivation for entity A

Input: Elliptic curve domain parameters p, a, b, n, G, the secret keys a, c, and the public keys S, T, U, V

Output: A secret point K E shared with the entity with public static key T

```
1: m dlog2e (n)/2 {m is the half bit length of n}
2: uA ‹(ux mod 2m) + 2m {ux is the x-coordinate of U}
3: sA‹ (c + uA a) mod n {implicit signature}
4: vA ‹ (vx mod 2m) + 2m {vx is the x-coordinate of V}
5: zA ‹ sAvB mod n
6: K ‹sA _ V + zA _ T
```

In order to derive the shared secret K, entity A and entity B have to accomplish an operation of the form k Æ P + l Æ Q (step 6 in Algorithm 1). This operation, which is called multiple point multiplication, has an impact on the overall computational cost of the ECMQV key exchange. This operation can be performed much faster when the doublings are combined as shown in Algorithm 2.

Algorithm 2: Multiple point multiplication

Input: The points P, Q E, scalar k = (km_1,. . . k1, k0)2 and scalar

l = (lm_1. . . l1, l0)2

Output: R=k_P+l_Q

```
1: Z ‹P+Q
2: R O
3: for i from m _ 1 down to 0 do
4: R ‹R+R {point doubling}
5: if (ki = 1) and (li = 0) then R ‹ R + P end if
6: if (ki = 0) and (li = 1) then R ‹ R + Q end if
7: if (ki = 1) and (li = 1) then R ‹ R + Z end if
8: end for
9: return R
```

3.2 Efficient combined security system

A wireless sensor network can be divided into several clusters. Each cluster has a number of sensors nodes and one of the nodes is elected as the coordinator (head). The energy analysis of the Kerberos protocol is based on the assumption that entity

A can directly send/receive messages to/from the third party T. This is reasonable for small sensor networks, but not for large networks where the sensor nodes may be located apart from the base station. The communication energy cost of Kerberos depends on the transmit power level and on the number of intermediary nodes between A and T. Multi-hop communication between A and T increases overall energy consumption since any intermediary node has to forward the message to its neighbor located on the route to the final destination. The Lightweight Kerberos intermediary node lies between them. On the other hand, ECMQV requires less energy protocol is more energy efficient than ECMQV when A can directly communicate with T or when at most one than Kerberos if there is more than one hop between A and T, which is always the case in large sensor networks. So, there is a need for system that compromise between the two protocols. That system is supposed to take the advantages of the two protocols and limits their shortening. The suggested system in this paper combines the using of the protocols in the same network in the following way: the network is divided into three layers. The first layer is 1-hop layer, means the nodes in this layer can communicate directly with the base station, it contains the base station (the sink) and clusters heads. The second layer is 2-hop layer and the third one is 3-hop layer, these two layers contain the ordinary sensors that belong to clusters. Lightweight Kerberos protocol with short messages is applied on the small network and ECMQV protocol on the large one. When sensors in layer 2 want to communicate with layer 1 they will use the Lightweight Kerberos protocol with short messages.The architecture of the combined system will be as in Fig. 2. The benefits of combining the two protocols in this system are as the following:

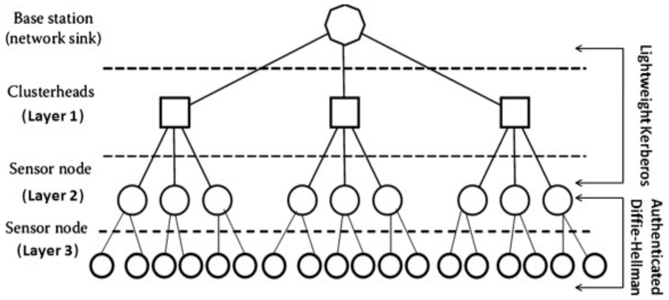


Fig. 9: Hierarchical architecture for the combined system

- Benefits of using Lightweight Kerberos protocol with short messages on layer 1 and for communication between layer 1 and layer 2.

The Lightweight Kerberos protocol is more energy efficient when the node is within direct communication to T (in most cases the base station) which is the case in layer 1 or when at most one intermediary node lies between them which is the case in layer 2.

- Kerberos does not need extensive computation so, it save the energy on the heads which is critical to these nodes because they are responsible for the general mission, collecting the sensed data of other nodes and routing to the sink.
- The number of heads and their neighbors is relatively small, so the total number of Kerberos communication messages will be relatively small. So, conserving the total energy of the network. For that, Kerberos is preferable in the small networks.

Benefits of using ECMQV protocol among sensor nodes in layers 2 and 3:

- ECMQV requires less energy than Kerberos if the communication between the node and T passes through more than one hop, which is the case in layer 3.
- The sensor nodes do not do additional tasks as heads, so they have some energy to do the computation of ECMQV protocol.
- The number of nodes in the two layers is relatively large and ECMQV is reasonable for large networks.

The number of communication messages needed for this protocol is small so improve the power consumption of the network.

Using two strong protocols as Lightweight Kerberos and ECMQV will improve the network security.

- Using the two protocols increase the speed of the network. This speed is drawn from:
- Using Kerberos in layer 1 and for communication between layer 1 and layer 2 reduce the number of calculation related to using ECMQV instead.
- Using ECMQV among sensor nodes in layers 2 and 3 reduce the number of communication related to using Kerberos on this large number of sensor nodes.

All these benefits will be gained by using the combined system and the results in experimental results section support that. Unfortunately, switching between the two protocols in layer 2, using Kerberos for communication with layer 1 and ECMQV for communication among nodes in layer 2 and for communication between layer 2 and layer 3, cause some load in this layer. But comparing to the saving in the power and enhancing the security it can be used.

4. CONCLUSION

The main purpose of this paper is to provide secure data communication among sensor nodes. The proposed model uses Kerberos authentication services in clustered sensor network. This will help to detect unauthorized objects in cluster itself rather than detecting it in complete network. On implementing Kerberos technique in every cluster will save the time as well as will improve the lifetime of the sensor nodes in wireless sensor network. Future work will include the implementation of this proposed technique in every possible scenario.

This paper presented combined security system combines Lightweight Kerberos and ECMQV Protocols. The combining system takes the benefits of the two protocols. One of system benefits is enhancing the energy consumption. Saving energy means decreasing number of communications and computations, and this improve the speed of the network. Another benefit is, using two strong protocols as Lightweight Kerberos and ECMQV improves the network security. The experimental results of the system compared with energy cost of Lightweight Kerberos and ECMQV Protocols showed that, the overall energy cost of using the combined system is less that using of Lightweight Kerberos or ECMQV alone. These results are based on the energy characteristics of the WINS sensor node.

5. ACKNOWLEDGEMENT

My sincere gratitude to my Head of the Department, Principal and Management for their valuable guidance and encouragement and providing sufficient infrastructure and facilities for me for my research work.

REFRENCES

[1] Kurose JF and Ross KW, Computer networking, a top-down approach featuring the internet, third edition.Addison Wesley, Reading, MA,2005.

[2] S. Jiang, N. Vaidya, and Wei Zhao, Dynamic Mix Method in Wireless Ad Hoc Networks. In Proc. IEEE Milcom, Oct 2001

[3] C. Shen, C. Srisathapornphat, and C. Jaikaeo, Sensor Information Networking Architecture and Applications,IEEE Pers. Commun., Aug. 2001, pp. 52–59.

[4] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, Security Issues in Wireless Sensor Networks, international journal of communicationsIssue 1, Volume 2, 2008

[5] K. Lu et al., A Framework for a Distributed Key Management Schemein Heterogeneous Wireless Sensor Networks, IEEE Transactions on Wireless Communications, vol. 7, no. 2, Feb. 2008, pp. 639-647

[6] J. Kohl, B. Neuman and T. Ts'o The Evolution of the Kerberos Authentication Service, in Brazier, F., and Johansen, D.Distributed Open System Los Alamitos, CA: IEEE Computer Society Press, 1994 networking.ACM Press; 2001. p. 189–99.

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

[8] Akyildiz I, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks. IEEE Commun Mag 2002;40(8):102–14.

[9] Sen J. A survey on wireless sensor network security. Int J Commun Netw Inform Secur (IJCNIS) 2009;1(2).

[10] Needham R, Schroeder M. Using encryption for authentication in large networks of computers. Commun ACM 1978;21(12):993–9.

[11] Kohl J, Neuman B. The Kerberos network authentication service (Version 5). Internet Engineering Task Force, Networking Group, Internet Draft RFC 1510; September 1993.

[12] Perrig A, Szewczyk R, Wen V, Culler D, Tygar J. SPINS: security protocols for sensor networks. In: Proceedings of the 7th annual international conference on mobile computing and

[13] Großsch J, Szekely A, Tillich S. The energy cost of cryptographic key establishment in wireless sensor networks. In: Proceedings of the 2nd ACM symposium on information, computer and communications security (ASIACCS 2007); 2007. p. 380–2.

[14] Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inform Theory 1976;22(6):644–54.

[15] Law L, Menezes A, Qu M, Solinas J, Vanstone S. An efficient protocol for authenticated key agreement. Des, Codes Cryptogr 2003;28(2):119–34.

[16] Raghavendra C, Sivalingam K, Znati T. Wireless sensor networks. Kluwer Academic Publishers; 2004.

[17] Singh K, Muthukkumarasamy V. Analysis of proposed key establishment protocols in multi-tiered sensor networks. J Netw 2008;3(6).

[18] Menezes A, van Oorschot P, Vanstone S. Handbook of applied cryptography. CRC Press; 1996.

[19] Neuman B, Theodore Ts'o. Kerberos: an authentication service for computer networks. <http://gost.isi.edu/publications/kerberos-neuman-tso.html>; 30 March 2012.

[20] Carman D, Kruus P, Matt B. Constraints and approaches for distributed sensor network security. Technical report #00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, USA;September 2000.

[21] Blake I, Seroussi G, Smart N. Elliptic curves in cryptography. Cambridge University Press; 1999.

[22] Blake I, Seroussi G, Smart N. Advances in elliptic curve cryptography. Cambridge University Press; 2005.

[23] Chen L, Lyu Z, Hong Z. An efficient cluster head selection strategy for wireless sensor network. In: Proceedings of the 5th international conference on genetic and evolutionary computing IEEE; 2011.

[24] 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.

[25] Raghunathan V, Schurgers C, Park S, Srivastava M. Energyaware wireless microsensor networks. IEEE Signal Process Mag 2002;19(2):40–50.

[26] Qin W. SimIt-ARM (Release 3.0). <https://sourceforge.net/projects/simit-arm/>; 30 March 2012.

Authors Profile

Prof. Pratik P. Bheley is an Assistant Professor it the Department of Electronics Engineering, Rajiv Gandhi College of Engineering and Research, Nagpur (MS) India. He did his M.Tech.(VLSI) from Shri Ramdeobaba College of Engineering & Management, Nagpur.,M.S. India. His research interest is in the area of Computer Networking, Embedded Systems.

Prof. Voore Subba Rao, is Sr.Executive Engineer, Systems Admin Dept. Adcc InfoCAD Ltd.,IT Park, Near VNIT, Nagpur. He did his M.Tech.(CSE) from JNTU, Hyderbad, India. His research interest is in the area of Computer Networking and Databases.