An Access control scheme based on ECC using ENABLE and HBQ Protocol for WSN security

Patil.S
Student/Department of E & TC
SKNCOE, Pune, India

Chilveri.P
Assistant Professor/Department of E & TC
SKNCOE, Pune, India

***Abstract*— Wireless sensor network (WSN) is cluster of sensor nodes that are densely arranged. For mission-critical related to wireless sensor network applications such as military and homeland security, health issues user's access restriction is necessary which provided by access control mechanisms for different access rights. Due to privacy reason or security clearance (i.e., a status granted to individuals allowing them access to classified information), user's access restriction may be enforced with different access rights .The introduction of a promising access control scheme based on elliptic curve cryptography (ECC). This system presents an energy-efficient access control scheme based on ECC to overcome limitaion of security and more importantly to provide dominant energy-efficiency. Analysis and simulation based evaluations proved that proposed scheme overcomes the security problems and has better energy-efficiency compared to current scheme.**

Index terms - User access control, Wireless sensor network (WSN), Elliptical Curve Cryptography (ECC), public-key cryptography, NS2.

I. INTRODUCTION

A wireless sensor network (WSN) commonly consists of a large number of sensor nodes that are densely arranged. It can sense physical phenomena or detect from the surroundings, process and provide the data to authenticated users. But it needs a lot of security, so cryptography is a most efficient technique used for security of WSN. A simple but efficient way is to rely on popular asymmetric-key cryptography rather than symmetric key cryptography because it has many disadvantages such as low scalability, requires large memory, difficulty to add or revoke key. An access control scheme based on ECC can be used for cryptography. According to analysis carried out it has been proved that the cryptography is more feasible as compared to symmetric key cryptography. One of the protocol introduced in this paper is Hop Based Queuing (HOP) which is introduced as a promising access control approach based on public key cryptography, but it has several limitations as follows [1]. It adds delay and consumes more energyIt fails to provide mutual authentication. It is vulnerable to denial-of-service (DoS) attack.

An Energy-Efficient Access Control Scheme Based On Elliptic Curve Cryptography (ENABLE) is implemented. ENABLE achieves better energy-efficiency than HBQ, and almost similar to symmetric-key based approaches.

II. RELATED WORK

The WSN basically needs high level of security which can be given to it different techniques like cryptography. Cryptography is one of the techniques which are the most reliable one.

A. Cryptography

For mission critical application such as military applications, health monitoring. The sensor networks are being used for varieties of applications military sensing and tracking, patient monitoring, and environmental monitoring, and airport and home security. According to the property of sensor devices, the data of sensor network can easily be modified messages or provide misleading information to other sensor nodes.

To prevent information and communication systems from illegal delivery and modification, the message is to be authenticated by receiver and transmitted from the sensor nodes over a wireless sensor network. So, there is need of technique that provides an authorization and authentication to this wireless sensor network. This is done by providing access control scheme which includes authorization and authentication steps [12] security purposes and to provide security to wireless sensor network.

B. Cryptography Algorithms

There are a number of image fusion algorithms which mainly perform basic operations like pixel selection, addition, subtraction or averaging. The different fusion algorithms are described below.

1] Improved authentication

An improved user authentication protocol by Rakesh Mahrana [11] scheme based on Elliptic Curve Cryptography (ECC) has been introduced for wireless sensor networks (WSN). . This scheme implements merit of using ECC based mechanism in WSN and enhances the WSN authentication with higher security than other protocols.

2] TinyPK

The design and implementation of public-key (PK)-based protocols that allow authentication and key agreement between a sensor network and a third party as well as between two sensor networks [12]. The disadvantages are that mutual authentication and secret session key is not provided.

3] Two factor authentication

Two factor authentication is given by Khan and Alghathbar [13]. This protocol has an advantage of introducing password change phase, protection against insider attack, overcoming GW-node bypassing attack and providing mutual authentication.

4] HBQ (Hop Based Queuing)

The disadvantages are that it is burdensome for sensors, it does not provide mutual authentication and it is vulnerable to DoS attacks [1]. The HBQ is a novel active queue management technique for ad hoc networks is proposed, where the dropping probability depends on the number of wireless hops traversed by the enqueued packets in the node.

5] ENABLE

ENergy-efficient Access control scheme Based on eLliptic curvE cryptography (ENABLE) [1]. ENABLE retains all advantages of public key cryptography and also enhances the security of HBQ.

III. OBJECTIVES & OVERVIEW OF THE PROPOSED MECHANISM

In this paper, the ECC (Elliptical curve cryptography) technique is used for providing security for wireless sensor network. The two protocols are implemented and results are compared on ns2 simulator.

A. HBQ protocol

HBQ is abbreviated form of Hop Based Queuing which is a protocol used for cryptography .It is type of public key cryptography used for authentication purpose. A user needs to apply for access permissions from a key distribution center (KDC) to access the network. KDC maintains an Access Control List (ACL) pool and associated user identifications. User's access privileges are defined in an ACL that is typically composed of user identifier (uid), group identifier (gid), and user access privileges mask. The user access privilege mask is a set of binary bits. Each bit represents permission of a specific information or service [1]. The algorithm is described as follows.

Algorithm Description: Algorithm is described in detail in the following table. The line by line description of algorithm is very important for writing further codeThe algorithm gives proper description of HBQ Protocol.

Our algorithm description is summarized in table 1.

EQUATION	DESCRIPTIONS
Alice → sl : TA = (CA||acA)	KDC issues proper ACL (aC_A) and attaches it to public constructor (C_A) as a certificate.
sl computes: QA = eACA + Q	Signature e_A is generated for ACL and KDC constructs the public key Q_A
picks a random r ∈ GF(q)	Sl selects a random no. r and calculates its signature H(r) over mod (q).
Zr = H(r)QA	Zr session key is generated
Yr = H(r)P	Temporary public key Yr
zr = r ⊕ (Zr)	Sl encrypts the session key by computing r modulo two addition with (Zr)
MAC(r,NA)	attached with message authentication code(MAC)of nonce(N_A)
Sl → Alice: zr,Yr,MAC(r,NA)	Sl sends a cipher text (zr, Yr) to alice
Alice computes: qAYr = qAH(r)P = Zr	Alice regenerates Zr
r = X(Zr) ⊕ zr	Alice decrypts the session key r
decrypts MAC(r, N_A)	R is used as sesson key to generate MAC value of nonce N_A
Alice → sl: MAC(r, N_A|| acA)	N_A concenated a_{CA} and sends to sl
sl → Alice: MAC(r, reply)	Sl decrypts the MAC message and verifies N_A and $a_{CA.}$ it is proved that alice is owner T_A

Step I - KDC issues proper ACL (aCA) and attaches it to public constructor (CA) as a certificate. Signature eA is generated for ACL and KDC constructs the public key QA and S1 selects a random no. r and calculate its signature H(r) over mod (q).

Step II - Zr session key is generated and temporary public key Yr is also generated. Sl encrypts the session key by computing r modulo two additions with (Zr). MAC(r,NA) attached with message authentication code (MAC) of nonce (NA).

Step III - Sl sends a cipher text (Zr, Yr) to Alice i.e Zr, Yr, MAC(r, NA). Alice compute qAYr = qAH(r)P = Zr and regenerates Zr. Alice decrypts the session key r decrypts MAC(r, NA) R is used as sesson key to generate MAC value of nonce NA. Alice sends NA concenated aCA and to sl. Sl decrypts the MAC message and verifies NA and aCA. It is proved that Alice is owner TA.

Disadvantages of HBQ: Although HBQ scheme introduces a promising access control approach based on public key cryptography, it still possesses several limitations as mentioned earlier.The disadvantages of HBQ are removed by using another protocol which is explained in further paper.

a) It is burdensome for sensors

As the authors discussed in their paper the authentication takes about 10.1 s and consumes 54.5 mJ for computation only. This means that HBQ scheme takes 130 times longer in authentication time and 80 times more expensive in energy consumption than symmetric-key based schemes. This makes HBQ scheme not feasible to be employed in practice.

b) It does not provide mutual authentication

In the scheme, Alice authenticates to sensor sl, but sl does not authenticate to Alice. In many cases, it is necessary to authenticate sensors to ensure that Alice receives correct information from a legitimate node. As an example, consider a battlefield scenario where the officer wants to make sure that detecting an alert of an enemy tank must be originated from a legitimate node.

c) It is vulnerable to DoS attacks

In the second step, upon receiving TA from Alice, sensor sl must perform three ECC point multiplications, one XOR, and one symmetric encryption. Each ECC point multiplication on TelosB mote 8 MHz takes 3.5 s and consumes more energy. An attacker could easily have a DoS attacks by sending a forged TA to sl and could rapidly deplete sl's energy.

B. ENABLE protocol

ENABLE is abbreviated as An Energy-Efficient Access control scheme Based on ECC is used to overcome the limitatios of HBQ and more importantly to provide dominant energy-efficiency is public key cryptography protocol based on access control [1]. It provides Mutual Authentication, it can defend against Replay Attacks, and it can defend against DoS Attack (Denial of Services).

Disadvantages of HBQ: The algorithm is described in tabular form for better understanding of the working of the protocol. The algorithm only defines the basic operation of this ENABLE protocol which is very helpful for writing code in NS2.

The algorithm description is summarized as follows in table 2.

EQUATION	DESCRIPTION
Alice computes: $L = h(x_A \oplus T_A)$	Secret key L is created (T_A is current timestamp generation by alice)
s_1= signA((r)L||certA)	Encrypts r with key L,(r) L Alice signs this encrypted value along with its certificate (s_1).
Alice → S: (r)L, T_A, s_1	This is send to sensor S
S computes: MAC_1 =MAC(xS, (r)L|| T_A || s_1)	S first checks T_A is Valid. If yes ,it builds MAC by shared key x_s (MAC_1)
S → KDC: (r)L, TA ,s_1, MAC_1	The sensor then forwards the message along with MAC_1 value to KDC
KDC checks if T_A is valid	KDC verifies T_A
verify(MAC_1), verify(s_1)	KDC verifies MAC_1 and s1 is verified
verify(certA), $L = h(x_A \oplus T_A)$	If signature is also verified alice is authentic .The certA certificate is also verified to check the validity o access list (ac_A).
r = decrypt((r)L)	(r)L is decrypted to get r.
$M = h(x_S \oplus T_{KDC})$	Secret key M is generated (T_{KDC} is timestamp generated by KDC)
MAC_2 =MAC(xS, (r)M||I_{DA}))	R is encrypted ,and MAC is builds MAC_2
KDC → S: (r)M, T_{KDC}, I_{DA}, MAC_2	(r)M, T_{KDC}, I_{DA}, MAC_2 are sent to sensor.
S checks if T_{KDC} is valid?	whether T_{KDC} is valid or not.
verify(MAC_2)	MAC_2 is verified
$M = h(xS \oplus T_{KDC})$	Secret key M is constructed
r = decrypt ((r)M	(r) M is decrypted to get r.
MAC_3= MAC(r, IDS)	MAC_3 is generated
S → Alice: MAC_3	After receiving MAC value from S, alice verifies same key by r.
Alice verifies (MAC_3)	S is authentic to user

Step I - Alice computes secret key L is created (TA is current timestamp generation by Alice). s1 Encrypts r with key L, (r) L. Alice signs this encrypted value along with its certificate (s1). This is send to sensor S. S computes and first checks TA is valid. If yes, it builds MAC by shared key xs (MAC1).

Step II - The sensor then forwards the message along with MAC1 value to KDC. KDC computes and checks if TA is valid. KDC verifies TA. KDC verifies MAC1 and s1 is verified. If signature is also verified Alice is authentic .The certA certificate is also verified to check the validity o access list (acA).

Step III - (r) L is decrypted to get r. Secret key M is generated (TKDC is timestamp generated by KDC) MAC2

=MAC (xS, (r) M||IDA)). R is encrypted, and MAC is builds MAC2. KDC → S: (r) M, TKDC, IDA, MAC2(r) M, TKDC, IDA, MAC2 are sent to sensor. S computes and checks if TKDC is valid? Checks whether TKDC is valid or not and verify (MAC2). MAC2 is verified. M = h (xS ⊕ TKDC), Secret key M is constructed, r = decrypt ((r) M and (r) M is decrypted to get r.

Step IV - After receiving MAC value from S, Alice verifies same key by r. Alice computes and verify (MAC3) S is authentic to user.

Advantages of HBQ scheme: The HBQ protocol have number of advantages like mutual authentication, defends the replay attacks and also DoS attacks.

a) It provides mutual authentication

KDC verifies the signature S1. If S1 is valid, then the user is authentic to KDC because only the user can generate the signature S1 by his private key [1]. Consequently, the user is also authentic to sensor S because S trusts KDC.

b) The Proposed Scheme Can Defend against Replay Attacks The adversary can intercept the message sent out from Alice (step I) or from the sensor S (step I). However, both cases are not possible in ENABLE because KDC can easily detect by verifying timestamp TA (step III).

c) The Proposed Scheme Can Defend against DoS Attack

Upon receiving the message from the user, the sensor first checks the timestamp TA if it is valid. It then builds a MAC using a very fast Message Authentication Code algorithm such as CBC-MAC and forwards the message to KDC. The proposed scheme significantly reduces DoS compared to HBQ.

Hardware Requirements: The hardware requirements are mostly sensors. MICA mote is one of such sensor.

1) MICA2 mote

The hardware used in this proposed mechanism was a selection of MICA2 Motes from Crossbow Technology Inc2. The Motes are model MPR400CB which uses the CC1000 900 MHz data radio. The sensor boards which were used are the MTS300CA which enables the mote to measure temperature, sound and light in addition to the battery voltage (used to power the Motes). The base station interface unit, model MIB510CA, is RS232 based and serves two main purposes (1) It allows the user to reprogram any mote by plugging the mote directly into the base (2) operates as part of the root node interface giving the PC a data conduit onto the radio based sensor network.

The MPR400CB is based on the Atmel ATmega 128L. The ATmega 128L is a low-power microcontroller which runs TOS from its internal flash memory.

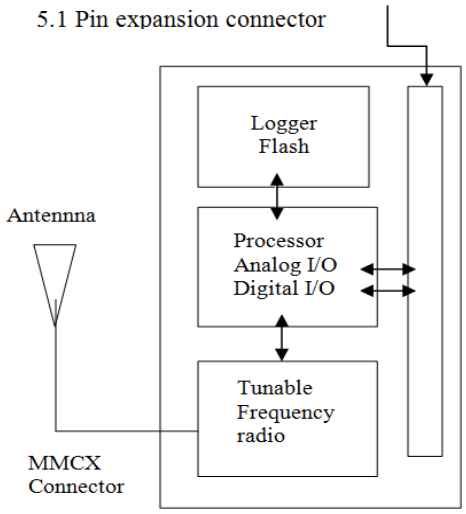

Figure 1. MPR400CB Block Diagram

Using TOS, a single processor board (MPR400CB) can be configured to run sensor application/processing and the network/radio communications stack simultaneously. The MICA2 51-pin expansion connector supports Analog Inputs, Digital I/O, I2C, SPI, and UART interfaces.

1)MTS101CA Photocell/ Thermistor/Proto and

2)MTS300CA/MTS310CAPhotocell,Thermistor, Microphone,Sounder, Magnetic (310 only), Acceleration (310 only)

The sensor boards connect to the MICA2 through a surface mount 51-pin connector. Crossbow supplies the above sensor boards.

Software Requirements: The software and operating system to operate the sensors. The simulating tool is also required to validity and feasibilty of protocol before actual implementation.

1) TinyOS 1.0

TinyOS 1.0 is a small, open source, energy efficient, software operating system developed by UC Berkeley which supports large scale, self-configuring sensor networks.The operating system is freely available so it is very cheap for use.The TinyOS 1.0 is very flexible as compare to other operating system and it is easy to use.

2) Network simulator (NS2)

The source code and software development tools are available freely and for simulation NS2 is used. NS2 is simply an event driven simulation tool that is used in studying the dynamic nature of communication networks. Simulation of wired as well as wireless networks protocols and function for e.g. routing algorithms like AODV, TCP, UDP can be done using NS2.NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors and therefore it gives better simulation results as compare to simulink.The results can be plotted in graphical format which is easy for concluding the results.The software are affordable as compare to hardware. They are available free of cost. The code can be written in C++ in NS2 installed on any virtual machine mostly LINUX.

V. PERFORMANCE EVALUATION

A. *Simulation Model and Parameters*

This section presents the performance evaluation of HBQ protocol which includes the computational delay and energy consumption. The throughput means rate at which data is transffered in certain amount of time is shown by using graphs. In these paper, the proposed protocols HBQ is implemented on Network simulator (NS2). The total of default 50 nodes is used for formation of wireless sensor network (WSN).

The simulation settings and parameters are summarized in table 3.

Parameter	Value
Simulator	NS-2.34
Radio Propagation Model	Two Ray Ground
MAC Type	802.11b
Interface Queue Type	DropTail
Link Layer Type	LL
Antenna	Omni Direction Antenna
Max packet in queue	200

B. *Performance Metrics*

The evaluation is mainly done by considering the performance according to the following metrics.

Energy: The average and total energy consumption is considered for nodes to determine the energy of wireless sensor network.

Delay : The delay is averaged over all nodes and considered for evaluation.

Throughput: It is rate at which data is transferred. The throughput is also considered as one of the importanat factor.

Packet Delivery Ratio: The ratio of sent and received packets is calculated.

The simulation results are presented in the next part.

C. *Results*

Figure 2 shown above shows how the simulation of network when HBQ is applied. The simulation windows shows actual data transfer between nodes. The step size kept here is 125.9µs, so that the simulation can be easily viewed. The Fig. 2 represents actual simulation of nodes; it means that data packets sent and received can be viewed in this simulation window. The simulation can be run, stop or paused.

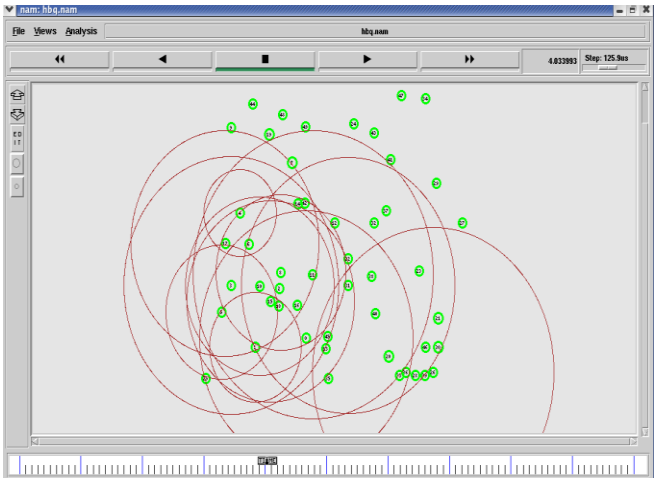

Figure 2. Simulation Window

The Fig. 3 shows the energy graph is considered as the important parameter used in analysis of WSN. The x-axis represents no.of nodes and y-axis plots average energy consumed by nodes.The parameter mentioned above is energy consumption, which can be used to conclude that HBQ protocol can be used for WSN security.The HBQ is access control mechanism based on ECC (Elliptical Curve Cryptography) technique which is used for security because it is easy to encrypt and decrypt the data.

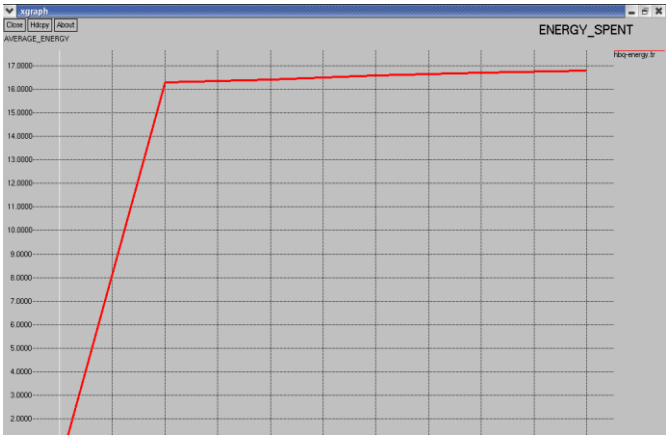

Figure 3. Performance evaluation based on energy consumption for HBQ Protocol

The throughput, packet delivery ratio and delay are others different parameters can be used for detail analysis. As always a coin has two sides, alongwith the advantages HBQ faces some disadvantages. Th disadvantages such as DoS attacks are very vulnerable, time consumed is more as compared to symmetric key technique and most important the mutual authentication is not provided in HBQ which is very important for security purposes.

VI. CONCLUSION

In this paper, the protocols HBQ are simulated on NS2 and the disadvantages are highlighted. The simulated

results are seen on NS2 simulator which gives analysis for further comparison. The next step is to simulate ENABLE protocol and compare both protocols by considering some parameters and to analyse how ENABLE overcomes limitations of HBQ protocol. The HBQ results can be further compared with the ENABLE protocol. The parameters like throughput, energy consumption, delay etc which are mentioned above can be used for comparing protocols.The comparison can be done by adding some additional parameters like packet delivery ratio (PDR), throughput, delay etc.

REFERENCES

[1]. Xuan Hung Le, Sungyoung Lee, Ismail Butun, Murad Khalid, Ravi Sankar, Miso (Hyoung-IL) Kim, Manhyung Han, Young-Koo Lee, and Heejo Lee "An Energy-Efficient Access Control Scheme forWireless Sensor Networks based on Elliptic Curve Cryptography" Journal of Communications And Networks, Vol. 11, No. 6, December 2009.

[2]. Rakesh Maharana, Pabitra Mohan Khilar "An Improved Authentication Protocol for Hierarchical Wireless Sensor Networks using ECC ", International Journal of Computer Applications (0975 – 8887) Volume 67– No.22, April 2013, pg no 23-30.

[3]. Ronald Watro, Derrick Kong, Sue-fen Cuti, Charles Gardiner, Charles Lynn1 and Peter Kruus "TinyPK: Securing Sensor Networks with Public Key Technology" October 2004, Proceeding of the 2nd ACM workshop on Security of adhoc and sensor networks SASN '04, Publisher: ACM Press.

[4]. Muhammad Khurram Khan and Khaled Alghathbar "Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks", ISSN 1424-8220, pg no 2451-2459.

[5]. Teerawat Issariyakul, Ekram Hossain "Introduction to Network Simulator NS2" ISBN: 978-0-387-71759-3 e-ISBN: 978-0-387-71760-9, DOI: 10.1007/978-0-387-71760-9.

[6]. Xiaowang Guo , Jianyong Zhu "Research on Security Issues in Wireless Sensor Network "s, 2011 International Conference on Electronic & Mechanical Engineering and Information Technology, pp.636-639.

[7]. Asha Rani Mishra, Mahesh Singh "Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network", International Journal of Engineering Research & Technology (IJERT),Vol. 1 Issue 3, May - 2012, ISSN: 2278-0181,pg no 1-6.

[8]. Fundamentals of Wireless Sensor Networks: Theory and Practice.

Authors Profile

S.Patil received the **B.Tech.** degree in electronics and communication engineering from the Department of Technology, Shivaji University, Maharashtra, India, in 2012. Currently doing **M.E.** in VLSI and ES from University of Pune, Maharashtra, India. Her research interest includes wireless communication (**WiFi,WiMax**), Mobile Ad hoc networks ,Sensor Networks, Communication networks

Paste Photo here

P.Chilveri received the **B.E.** degree in electronics and communication engineering from the PVG, University of Pune, Maharshtra, India, in 2001. Completed **M.Tech.** in electronics and communication engineering (Applied electronics) from College of Engg, Pune, Maharshtra, India. His research interest includes wireless communication (**WiFi,WiMax**), Mobile Ad hoc networks ,Sensor Networks ,Neural Networks and fuzzy logic, Communication networks