Current Trends in Technology and Sciences
ISSN : 2275-0535
9th Symposium on Advances in Science & Technology (9thSASTech 2014), Mashad, Iran

Increasing the Security of SCADA Systems using Key Management and Hyperelliptic Curve Cryptography

Akram Ebrahimi
Islamic Azad University, Kerman Branch, Kerman-Iran, MSc Student in Computer Engineer.
aebrahimi.computer@gmail.com

Farokh Koropi
Islamic Azad University Kerman-Iran, Computer Engineering Department.
farokhkoroupi@gmail.com

HamidrezaNaji
Graduate University of Advanced Technology Kerman-Iran.
hamidnaji@ieee.org

***Abstract* – A SCADA system operates as a control center of a central termination which receives information from one or more remote terminals and issues commands to them. To increase the security of systems encryption can be used to protect data transfer and storage. In this paper, we have suggested a safe environment in SCADA networks to create a proper communication between control center and RTU using key management protocol, mutual authentication And digital signature. So the server can ensure the security and non-manipulation of received and sent data. For this purpose, we use Hyperelliptical curve cryptography. Hyperelliptical curve is so suitable in cases where we have power, storage and time limitations as it needs fewer calculations and parameters in compared to other cryptography schemes such as elliptic and RSA. for example, 80-bit space is required for the HECC field whereas in ECC, 180 bits and in RSA, 1024 bits are required.**

***Keyword* – SCADA, digital signatures, Hyperelliptical encryption, key management.**

1. INTRODUCTION

Modern industrial facilities such as electric power generating plants have command and control systems. These industrial command and control systems are commonly called Supervisory Control and Data Acquisition (SCADA) [1]. SCADA systems today can run on many platforms and are readily available to buy "off the shelf". This has reduced the cost of buying, installing and maintaining SCADA systems. As a result SCADA systems are today widely used to monitor and control critical system infrastructures. Modern SCADA systems are now complex and vast; far more so than their predecessors that relied on simple point-to-point networks. A modern industrial network can be divided into segments; a corporate network segment, SCADA network segment and field devices segment.

In June of 2010 the Stuxnet computer worm was identified by Belarus-based security firm, Virus BlokAda (Keizer, 2010). After analyzing the worm, experts have claimed that it is the first cyber weapon targeted at exploiting SCADA systems. In particular, it is claimed that the worm targets specific computer systems in Iran that are purportedly used in the creation of nuclear technologies. This Windows based worm specifically targets Siemens control systems and is able to covert and reprogram the programmable logic controllers (PLC). Experts have highlighted that the worm is highly sophisticated, exploiting a total of 5 zero-day vulnerabilities; this being another world first.

The details of the worm, such as its sophistication, identified targets and manner of operation, suggest that no individual, hacker or criminal group would have access to resources, or for that matter such a motive, in order to perform such a targeted attack. Experts state that further forensic analysis of the malware is likely to reveal the perpetrators.

The Stuxnet computer worm has highlighted the real threat of CW and has undoubtedly lead nations to seriously consider the security posture of their critical infrastructures. To date, Iran has made a number of arrests in relation to the Stuxnet computer worm [2].

Many researchers have proposed key management schemes for SCADA. However, previous studies lack the proper considerations for availability. Namely, they do not have a solution for when the main device has broken down. In addition, since many SCADA system devices are remote from the control center, they are physically insecure. Therefore, the devices need to periodically update the security keys which they store. However the computation and communication costs of this update process increase as both the number of vulnerable devices and keys increases, so SCADA systems need to reduce the number of keys transmitted for security and efficiency [1]. The need to keep the constraints such as computational capacity constraints, limited capacity, actual processing time, data transfer rate and low number of messages in mind, are required before creating a

secure mechanism for this system. Many efforts in the field of key distribution and key management are done to provide system secure, but there is still a scope for improvement [3].

In this paper, we propose Hyperelliptic curves over finite fields key management architecture for a robust SCADA system which supports the replace protocol for availability and reduces the length of keys to be stored in a master terminal unit (MTU). This is because in the proposed scheme, the algorithm is designed to find the discrete logarithm of a random element for elliptic curve with respect to a divisor. Therefore, the Hyperelliptical curve algorithm is designed on limited areas and finding the discrete logarithm of a random element is hard work, due to a divisor group against the elliptical curve that is known on a general basis point.

2. Related Works

A cryptographic key management and Key Establishment approach for SCADA (SKE) was proposed by Sandia National Laboratories in 2002, Their paper firstly outlines SCADA security systems architecture and then discusses a key management solution. However the key management design that Beaver et al have proposed, has the following limitations:1. Both symmetric and public key cryptography techniques are used. 2. Long term keys are shared between nodes via manual installation. If a Remote Telemetry Unit (RTU) has multiple master stations, its key will need to be installed on each master station. Also, if a master station is compromised, long term keys are also compromised [4].

Information Security Institute, Queensland University of Technology, Australia also proposed a Key Management Architecture for SCADA systems (SKMA). In this scheme a new entity 'Key Distribution Center (KDC)' was introduced, which maintains long term keys for every node [5].

Proposed a scalable key management scheme to improve the security and performance of SCADA networks. Kang et al. in 2009, investigated security problems in radial SCADA networks. They proposed a key management scheme for secure communication in SCADA networks. They also suggested a solution for the optimal key distribution period time. The electric power system is thought of as a typical model using the SCADA network for its remote control and monitoring. Kang et al. primarily addressed the unique security environment and inherent problems in the radial SCADA network of electric power systems. Their approach is informed by the symmetric encryption method. For the most part their paper is limited to the key management for encryption and provides a solution to the optimal key distribution period as well. They suppose that the communication in radial SCADA networks is made only between the master station and each RTU or IED. Kangetal's key management scheme, the master station takes the role of the KDC. This is implying that an additional KDC is not required [6].

Liangliang Xiao et al in 2010. Key management from KGS protocol, key distribution is performed before Development nodes and after the CA established Community uses the authentication protocol and The key update protocol and also add and delete nodes performs as Elliptic curve cryptography algorithm. in propose authentication scheme Each RTU can access to the other of the nodes while the network traffic increases [7].

Zia Saquib et al in 2011. The computation time and energy required by ECC and PBC based methods still exceeds the time and energy requirements of symmetric key schemes, which makes it difficult to use these schemes in scenarios where nodes have to frequently communicate with several different nodes in the cluster one after other. The proposed scheme uses Elliptic Curve Pairing Based Pairwise Key Establishment for bootstrapping the polynomial share based scheme and providing the flexibility to the network nodes to communicate with and authenticate outside the cluster if required. It has been shown that the elliptic curves based scheme is more expensive in terms of both time as well as energy and time consumption. So the use of ECC pairing based scheme should minimized as much as possible. But their scheme does not completely solve the problem as there is no surety of direct links and lack of knowledge of the network topology may lead to heavy communication overheads for pair-wise key establishment. Also, a number of un-compromised links is affected due to compromised nodes.

On the other hand, the public key schemes (RSA, Diffie Hellman etc.) do not suffer such problem. No uncompromised node is affected due to any compromised nodes in the network. But traditional public key schemes are too resource intensive and consume considerable amount of bandwidth and computation time. The studies specifically targeted to PKC have tried either to use conventional algorithms (e.g.RSA) to nodes or to employ more efficient techniques (e.g. ECC). There works show that ECC based schemes outperform RSA based schemes and are feasible for resource constrained nodes [8]. In 2013 Rezai et al propose a new key management scheme for SCADA networks based on a decentralized key distribution model which improves these conditions. In the proposed key management scheme, the session key generation devices are also displaced from the slave station, which has low computational resource, into the master station which has enough computational resource. Moreover, the master station has a time stamp to update the session key and master key. The proposed key management contains three phases: initial condition phase, session key update phase and master key update phase [9]. We are using the advantages of pairing based system such as easy key management and high connectivity and resiliency in the proposed scheme so as to make the proposed scheme easy to manage and provide high resiliency and connectivity. Since SCADA

networks are used for a long time so we need to a low-bandwidth communication line [10].

Therefore, it is necessary that the required connections between control center and RTU have been reduced in updating square key. Speed plays a major role in SCADA networks and delays in data processing in SCADA networks can be a serious problem. So the model of decentralized key distribution is proposed for such a situation. The tools of session key generation from remote terminal are displaced due to the low amount of computational resource to control center because they have powerful and sufficient computational resources. So, we use asymmetric encryption in the proposed scheme and because the encryption key is different from decryption and the computations of asymmetric encryption is much higher, the system square is higher. We compared these approaches and converted ECC approach to HECC, which is a key management approach of Rezai and Saquib and Xiao, since the Hyper-elliptical cryptography is performed on an 80 bit field. While the elliptic curve works well with the same level of security in 160-bit field and this effects the number of bits in the storage memory and communication bandwidth. Also in the key management of the proposed scheme, we have used the Digital Signature algorithms and production of session key and as a result, system is protected against the repeated attacks on SCADA networks. In section three SCADA and communication systems are introduced and in section four, the proposed approach of Hyper-elliptical curve algorithms is presented. Section five summarizes the proposed approach and conclusions are made.

3. SCADA System and Security Requirements

A SCADA system network is different from general network environment due to its operational environment in national infrastructure. Therefore, the network system has the following constraints.

1) **Limited computational capacity**: The remote equipment such as RTUs are embedded system having low computational and space capacity.

2) **Low data rate transmission**: Since the SCADA system have been used for a long time, the communication line of the SCADA network has low bandwidth.

3) **Real-time processing**: The SCADA system should behave accurately. Delay in data processing could cause serious problem.

Above constraints of SCADA systems make it difficult to apply the security technology to the system so that the constraints should be a basic consideration for applying security mechanisms [10].

There is no established security policy for Korean SCADA network since it has been recognized as a safe facility against external attacks until now. As stated above, the infrastructure is becoming the main destination of terrorism since the impacts incurred by such attacks are so huge. Cyber assaults are sure to cause the same system fault as physical attacks. The coordinated attacks on major power plants or substations may trigger a cascading blackout, resulting in severe social and economic damages [7].

For example, a computer hacker could destroy a transformer in substation by transmitting the signal of transformer overload, thereby causing it to rapidly overheat and explode as if a bomb were dropped or a fire broke out. Data Measurement and control signal are exchanged through the communication lines between RTUs and the master station as shown in Fig. 1. Assuming that there are no internal approaches from the inner parts of RTUs or the master station, one of possible methods to crack this system is to tap a communication line directly since this network is completely closed to other networks, allowing no detour to get access to the SCADA systems [6].

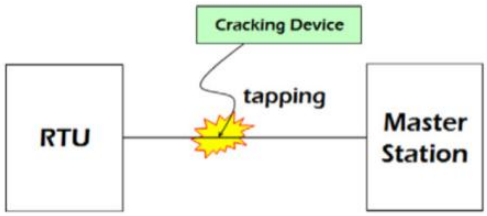

Fig. 1. Intrusion into the communication line [6].

4. Proposed Protocol

Current Research on HECC emphasize on finding efficient methods to select secure hyperelliptic curves, fast operations on the Jacobians and implementation of HECC for use in practical applications to enhance SCADA network security. The protocol of the proposed key management is simulated based on the Hyper-elliptical cryptography in SCADA network. These cases show the design improvements related to previous works: Key Management protocol based on HECDSA in SCADA network uses genus 2 HEC on 80 bit finite fields which achieve

the same security level as 160-bit ECC. Encryption of transmitted message using a symmetric encryption process saves energy and storage and reduction communication overhead**.**

In this approach, system protection is maintained against the repeated attacks on SCADA networks by creating session key in each period and because of the connection on both sides, session key is calculated separately, and it is secure against known key attacks. Key management protocol reduces the communication overhead and storage volume based on Hyperelliptical curves in SCADA networks, because the type 2 Hyperelliptical curve cryptography is used in a finite 80 bit field that have the same security level as that of elliptic curve which uses 160-bit space. To establish a secure hyperelliptic curve, its Jacobian should satisfy the following conditions:

Adleman et al [11] found a sub-exponential time algorithm to solve the [1]DL in the Jacobian of HEC of a big genus over a finite field. Curves of higher genera (preferably $g \leq 4$) are, therefore, not suitable for cryptographic use ($2g+1 < \log qn$).

To harden a cryptographic primitive against simple side channel attacks, we make the observable information independent of the secret scalar. This can be achieved by applying Montgomery's ladder for scalar multiplication. In this protocol, from 3 phases of initial situation of system the RTU registration is started in KDC and we used the communication between the control center and RTU and the step of creating session key which are described as follows:

4.1. level 1: system initialization Conditions:

Any remote user can obtain service from other users without registering each time with the KDC. They can transfer data after authentication.

New session key is established for each particular session to protect data which resists replay attack in SCADA network. The HCDLP[2] in J(*C*; qn) is: given two divisors D1, D2 defined on J(*C*, qn) over qn, to determine integer m such that D2=mD1, provided such an integer *m* exists [12]. Key Distribution Center(KDC) generates a random hyperelliptic curve C defined over p. Then KDC computes semi reduced Divisor D and the unique reduced divisor D'of the selected curve using Cantor's algorithm.

KDC also computes a point P = (x1,y1) which is a base point on the curve, a large prime number p and a prime divisor q such that *q* divides p-1. *p* contains the representation of all field elements of order n. Finally the following system parameters (p, C, D', p, q, D, n) are generated by KDC.

4.2. second phase: RTU registration on KDC list

As each RTU is added, messaging network sends it to network for registering in KDC. After KDC registration, the system allocates an ID to each RTU and sends the ID to each RTU. Now, KDC has a list including all RTUs with their IDs. After deployment stage, KDC encrypts this list with system parameters. Here, because the RTU information is unknown for the key distribution center, no attacker can identify RTU unless it has ID of RTU and this is impossible due to Digital Signature.

[1] Distributed Logarithm
[2] Hyperelliptic Curve Discrete Logarithm Problem

Current Trends in Technology and Sciences
ISSN : 2275-0535
9th Symposium on Advances in Science & Technology (9thSASTech 2014), Mashad, Iran

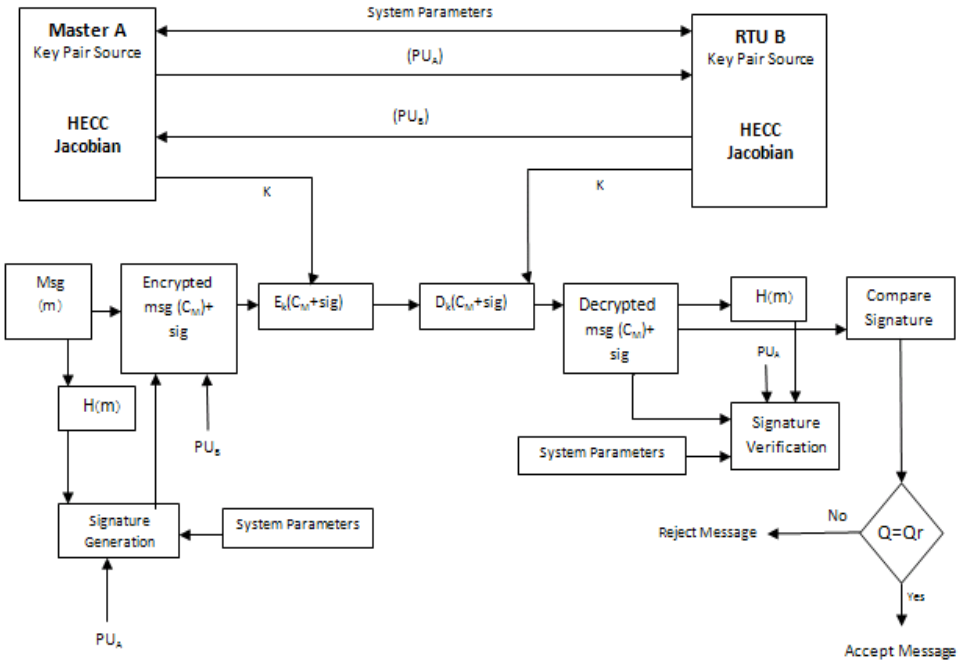

Fig. 2.The control center and RTU communication with encryption HECC

4.3.third Phase: the RTU communication and cotrol center with encrypted message

now, conrol center want to comminicate with target RTU so it sends a request mesaage to cotrol center to RTU included current ID_a and N_1. RTU receives a message if the user communicate with control center, so the target RTU sends an acceptable message to control center included of current ID_a, N_1. Now, the user of center station and RTU will communicate with each other after authentication. So, authentication approach is provided and it is shown in Fig. 2.

5. CREATION OF SESSION KEY

In this approach, session key is created with each step:

Step 1: RTU side

- It chooses d_B randomly that is $d_B \leq n-1 \leq 1$ and it calclutes $Q_B=d_B*D$.
- Then, it creates PR_B private key and PU_B $[PR_B]D$ public key.
- Finally, RTU sends $(Q_B$,$PU_B)$ to the control center.

Step 2: control center side

- It chooses a random d_A which is in the $d_A \leq n-1 \leq 1$ bound and then it calculates $Q_A=d_A*D$.
- Then, it calcultes $Z = a_A \oplus a_B$ for two-directional authentication.
- It creates the control center of priavte key PR_A and public key PU_A-$[PR_A]D$,for itself.
- After that cryptography key, $K=d_A*Q_B$; $r = (\sum_{l=0}^{e-1} L(V_1) g^i) \bmod p$; that e is an integer e<=g so $0 \leq L(V_1) < g$ (for mapping between jacobian j(fp) and limited field GF(P) also itcalculates $S = [r^{-1}(H(M) - PR_A]\ r\ )]$ for Digital Signature.

step 3: at RTU side, following cases are calculated:

- It calculates $B = Q_A \oplus Q_B$ and secure key $K=d_B*Q_A$; and if protocol works correctly, both users will create a similar k and by simple mathematical calculations, the formula (1) is proved:

  (1) $K=d_B*Q_A=d_B*d_A*D=d_A*d_B*D=d_A*Q_B$
- $W=(S)^{-1}$ is calculted and(ŕ,ś) is the received signature at the RTU side.
- After that, it calculates mod p, $u_1=(H(M)W)$, $u_2=(ŕ,w)$ mod p;
- In addition, it calculates V = [U1] D⊕[U2] PR_A.
- If we have v=[1,0], it shows a wrong signature and RTU rejects the signature with massage,
- It calculates $v' = (\sum^{l-1} l(v_{f,i}) q^i) mdf$ (for mapping between jacobian $J(F_P)$ and limited filed GF(P)) if we have (v̀==r) it shows a correct signature so the RTU verify the control center and RTU verifies that this key is a secure.

So, the control center verifies RTU and RTU similarly verifiesthe control center. Finally control center and RTU have a session key K_S which compromisesof $k_s = H\ (ID_S)(ID_B)(K\ )$ relation.

6. Evaluating the Proposed Approach

Hyperelliptical curves are suitable when we have limitations on the size of hardware operations such as power, time and storage. In order to protect networks from cyber active and passive attacks, we need varied and updated key methods. On the other hand, another security issue can be this that the server must ensure security and not manipulation of keys and messages and receive and send information. For this purpose, a digital signature is proposed. However, as the key length increases the decryption time increases too. For this purpose, systems and networks based on hyperelliptical curves, due to necessity the smaller operation than elliptic curves and RSA are recommended because they have high security. It should be noted that for final agreement of session key, we should established a key agreement protocol. The proposed protocol forces the users to develop public keys through third party, and which are validated. But in turn, this issue leads to increased energy usage and network traffic. For solving this issue, protocols such as Defi-Helman are used.Generally, the above system can be divided 1- initialization phase and 2- encryption key generation, 3- signature generation and verification and 4-cryptography and decryption. Table (1) shows the comparison between Hyperelliptical encryption algorithm with other elliptic algorithms and symmetric algorithms DES. As we can see, the Hyperelliptical algorithms include less execution time compared with elliptical curve.

Table (1) execution time of different complexity.

algorithm	DES in CBC mode	ECC in CBC mode	HECC in CBC mode
Execution time(second)	0.0056	0.0038	0.0037

Table (2) time in each step in algorithm of Hyper elliptical curves of second type 80-bits in binary filed

step	Execution time (Microsecond)
Curves Generation	66
Divisor Generation	171
Public Key PUA	256
Public Key PUB	275
User-A Secret key	199
User-B Secret key	187
Encryption	1289
Decryption	739
Signature Generation	506
Signature Verification	74

In the proposed scheme, QoS=PI+SI where PI indicates the performance and SI security indexes. As it is shown in Fig. 3, due to using asymmetric cryptography and having the minimum key length, it is increased substantially and traffic is reduced and QOS is increased. Gradually, by increasing the communication and traffic load of QoS and due to the bandwidth of connection period, it reaches a constant value.

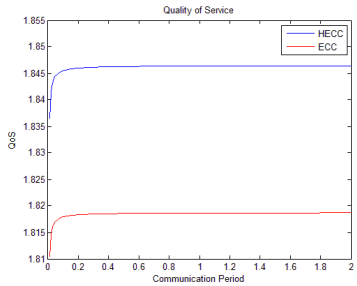

Fig. 3.changes in service quality in terms of the communication frequency per second.

An other important parameters in SCADA networks is the upgrade key. To establish a secure connection between two points, it is required for the session keys to change them. The time for change is often so great that the public key is not included in the calculations. Does not change the session keys periodically at fixed intervals SCADA system will lead to a sharp reduction in information security. For this reason, it is of interest that are updated frequently and quickly done. However, the rapidly changing session key is to reduce the band width to send and receive data and ultimately reduce the quality of service despite increase Channel-security. As seen in Fig. 4, quality of service by increasing the frequency of Key Distribution Period (number of updates per second) will be reduced Extremely. So by choosing an appropriate value for the frequency of updating the session key can be a proper balance between security and quality of service channels, established.

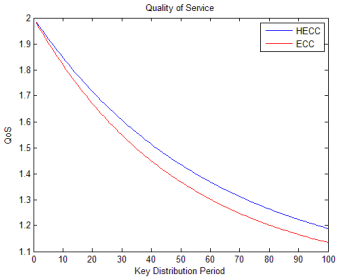

Fig. 4.shows the changes of service quality by key Distribute Period

7. Security Analysis

In this scheme, even if the enemy ID is compromised, it will never allow the enemy to determine the session key for past the session and their decoding and in this protocol, it is assumed that the problem is a robust discrete logarithm. If the attacker knows the accuracy ofQ_B but he can not calculates the previous session keys becauseK_S is derived from K security key and it is formed from d_A و d_B values. On the other hand, any unauthorized malicious user, can send information over and over again. In this protocol, after each time period, T_s that is unknown for each malicious user, a session key will be created for encryption, so there is no possibility of

an attack. Among the protocol objectives, we can mention the following:

- **Unforgeability**:

These calculations are impossible for an attacker transmitter to find (r,s) because for production,
sender needs to know the private key of PRA, according to $S = [r^{-1}(H(M) - PR_A]\ r\ )]$. One attacker should know the sender's private key and the hidden K, which is impossible.

- **Non- Undeniable:**

These calculations are possible for a third party to resolve the disputes between sender and receiver in an event that sender denies the origin of the message. Each trusted third party can resolve the differences between sender and receiver in the proposed program by using the protocol.

8. Comparison Between the Performance of Proposed System with Related Works

8.1.Communications (RTU to RTU and MTU to RTU)

The Z. Saquib approach included all kinds of relations due to the RTU clustering and using the protocol based on WSN. The A.Rezai approach investigated only the communication between MS and RTU and by considering this point that both sides can generate key [9] .the approach of L. Xaio [8] can included all type of communication due to a mutual authentication

8.2.Key Distribution Center (KDC or CA)

The presence of key distribution center in key management system puts a heavy load on system whether as a KDC or CA.But since the SCADA systems are industrial and are very vulnerable, the presence of such centershave a direct effecton reliability and system security, table3.

8.3.Comparison of Authentication

In A,Rezaiapproacj only key management is used and in the Squib approach, their authentication is based on id-NIKDS so the user data are identified as a unit. Base on email address or IP which have a public key authentication and the fact that issuer certificate is not needed, a mathematical-based formula on the nonlinear proposed approach, due to this fact that RTU has limited storage space and on the other hand, authentication mutual protocol have limited storage filed for devices that have low key size. And according to table 3,we can conclude that our system outperforms than SCADA existing system.

Table (3) Comparison between the performance of proposed system with SCADA systems.

Reference	Number key	Authentication	Curves	communication	Key distribute
(2010) L.xiao.[7]	M+3	Yes	ECC	All-comunaicate	CA
(2011) Z.Saquib[8]	2	Yes	ECC	All-comunaicate	CA
(2013) A.Rezai.[9]	2	No	ECC	MS-RTU	KDC
(2015) Our Result	2	Yes	HECC	All-comunaicate	KDC

8.4. Hyperelliptic and elliptic curves cryptography

Using HECC increases the reliability and ensures secure communications and ultimately reduces key length and the number of storage keys in comparison with ECC. And as a result, it reduces traffic and increase speed and computational speed increases, and as a result, according to table 3, our system maintains higher security than other systems.

8.5. The number of keys in each RTU:

each RTU and stores a number of keys in itself and in SCADA system it is so important that the stored keys should be very low in compare with L. Xiao paper and it is a product of m1* m2. That each RTU of public keys stores all CA in itself and have its updating operations and its private key. In A.Rezai paper, the number of keys in each RTU is 2 and the number of key in control center n+1, where n is the number of RTU in our system. Two public and private keys are stored in each RTU. But we have low storage space due to the lower key length.

9. Conclusion

In this paper, an improved key management approach is used for SCADA networks using HECC which is implemented by agreement protocol of Defi-Helman based of Hyper-elliptical curve. It has a smaller key length than elliptic curve and can be called as asymmetric encryption protocol, HECC. It reduces the traffic and cost of computing and storage, and also using mutual authentication algorithms, it increases the security of system with some parameters such as privacy and unforgeability.

Reference

[1] Donghyun. Jeong,Hanjae. Won,Dongho andKim,Seungjoo. "Hybrid Key Management Architecture for Robust SCADASystems,"Journal of Information Science and Engineering 27. Pp, 197-211, 2011.

[2] Nicholson,A. Webber,S. Dyer,S. Patel,T. Janicke,H. "SCADA Security in the light of

Cyber-Warfare.Computers & Security,"vol, 31. Pages, 418-436, 2012.

[3] Ludovic, Pietre. Sitbon,Pascal. "Cryptographic Key Management for SCADA Systems,"Pages, 156–161, 2008.

[4] C. L. Beaver, D.R. Gallup, W. D. NeuMann, and M.D. Torgerson: Key Management for SCADA (SKE): printed at Sandia Lab, March 2002.

[5] obert Dawson Colin Boyd Ed Dawson Juan Manuel Gon alez Nieto: SKMA – A Key Management Architecture for SCADA Systems: Fourth Australasian Information Security Workshop AISW-NetSec , 2006.

[6] Kang, D. Lee, J. Kim, B. and Hur, D. "Proposal strategies of key management for data encryption in SCADA network of electric power systems,"International journal of electrical power and energy systems. doi:9.916/j.ijepes, 2009.

[7] Xiao, Liangliang.Yen, I-Ling. Bastani, Farokh. "Scalable Authentication and Key Management in SCADA," 16th International Conference on Parallel and Distributed Systems, 2010.

[8] Saquib, Zia. Batra,Ravi.Pal,Om. Nevangune, Ashwin. Patel,Dhiren and Rajarajan, M. "A Configurable and Efficient Key-Management scheme for SCADA Communication Networks,"International Journal of Research and Reviews in Information Security and Privacy (IJRRISP).Vol, 01.No, 2, June 2011.

[9] Rezai, Abdalhossein. Keshavarzi,Parviz. Moravej, Zahra. "Secure SCADA communication by using a modified key management scheme,"Electrical and Computer Engineering Faculty.Semnan University.Iran ISA Transactions 52 .Pages, 517–524 ,2013.

[10] Lee, S. Choi, D. Park, C and Kim, S. "An efficient key management scheme for secure SCADA communication,"In Proceedings of World Academy of Science.Engineering and Technology.Vol, 35. Pages, 457-463, November 2008.

[11] dleman,L. DeMarrais,J and Huang,M. "A subexponential algorithm for discrete,". logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields.Algorithmic Number Theory (ANTS-1).LNCS 877. Pp, 28-40, 1994.

[12] Menezes, A. Wu,Y and Zuccherato,R. " An elementaryintroduction to hyperelliptic curves", Technical Report CORR 96-19. Department of C&O, University of Waterloo, Ontario, Canada. November 1996.