Volume 5, Issue 10, October-2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Group Key Exchange Analysis in Sensor Networks

[1]Sravanthi Dagani, [2]Balajee Maram
[1] Department of CSE, M.TECH (CSE) Student, GMRIT, Andhra Pradesh, India
[2] Asst. Prof., Dept. of CSE, GMRIT, Andhra Pradesh, India

Abstract— In Wireless sensor networks, the security is the primary imperative in message transmission. For secure group based message transmission, shared-key provides secure transmission. This paper addresses an intriguing security issue in portable specially appointed systems that are element gathering key assention for key foundation. For secure correspondence, a gathering key must be shared by all gathering individuals. This gathering key ought to be overhauled when the current bunch individuals are leaving the system or new individuals are coming into the current system. In this paper, we propose a productive gathering key understanding convention. Here the thought is the gathering key is calculated and sends to all the nodes which are part of the group. For calculating gathering keys we are using Elliptic Curve key forms. This paper analyzes the performance of weierstrass curve, Edward curve, and Jacobin curve. These gathering keys ought to be changed when there are participation changes, (for example, when the present part leaves or the new part joins). By presenting gathering based approach, messages and key redesigns will be constrained in gathering. Consequently calculation burden is changed when the gathering key calculation in centralized or distributed. Both hypothetical and pragmatic results demonstrate that Edward curve is the best form for proficient gathering key understanding convention performs well for the key foundation issue in impromptu system regarding proficiency what's more, security. And we analyze in both centralized and distributed.

Keywords— Wireless sensor networks; Elliptic curve; Weierstrass curve; jacobian curve; Edward Curve;

I. INTRODUCTION

WSNs have become most interesting research area because of its useful inherent characteristics such as power, small volume, scalability of nodes, easy to use etc. Day by day, many usages of WSN applications in hostile environments are being needed for demand of today's world because of many natural disasters like earthquakes, flooding, Tsunamis and forest firing, etc. Currently, WSNs have provided usefulness to several important field areas such as environmental monitoring like flood and forest firing detection, industrial monitoring like status monitoring, medical like Body Sensor Network (BSN), military like reconnaissance of opposing forces and other monitoring systems like air, water and animals . Depending on applications used for WSNs, security is the biggest challenges in WSNs and security aspect is essential for WSNs before designing WSNs. The resource constraints and limitations make WSNs most challenging research area such as energy and vulnerable to lack security.

The limited factors of using sensor nodes are that they have limited battery power and less memory capacity. To control information access in a sensor environment only authorized node must know the key to disseminate the information that is unknown to the compromised nodes. The communication keys may be pair wise, or group wise, these keys to be updated to maintain security and resilience to attacks.

Key management is concerned with the generation and distribution of secret keys, and their life-time administration, including key revocation and re-keying. This topic is well researched in wired networks, and many protocols have been proposed, some of which are successfully applied in large-scale networks such as the Internet. For WSNs, no "one size fits all" approach has been found. A large number of protocols have been proposed that are finely tuned for certain scenarios. These approaches often rely on a large number of assumptions that limit their applicability, such as leveraging a certain factor that is only available in a small class of scenarios. An example of this is scenarios with fixed topologies, which eases the distribution of secret keys significantly. This abundance of available protocols exists because wireless sensor networks are highly heterogeneous in their scale, application requirements and needed security guarantees. Further, a number of additional factors make key management in wireless sensor networks particularly hard and incompatible to classic protocols from the wired world. We propose an effective gathering key understanding convention in wireless sensor networks. In huge and high versatility specially appointed systems, it is impractical to utilize a solitary gathering key for the whole system as a result of expense of processing in rekeying. So we isolate the bunch into numerous subgroups and every subgroup has its own subgroup key which is shared by all individuals from that subgroup. In every subgroup, one hub is chosen as a passage hub which is the controller among subgroups. Passage hub is chosen in view of the strength estimation of the hub and force level of the hub. Every passage hub in different subgroups shape an external assembles and creates an external gathering key.

II. RELATED WORK

There are numerous gathering key assent-ion protocols for giving security. [12] presents public key agreement protocol which is based on Diffie–Hellman key exchange, in which two parties jointly exponent-ate a generator with

random numbers, in such a way that an eavesdropper cannot feasibly determine what the resultant value used to produce a shared key is. Exponential key exchange in and of itself does not specify any prior agreement or subsequent authentication between the participants. It has thus been described as an anonymous key agreement protocol. [2]In the Multi-level group based key management protocol they not only share the private and public key but also uses higher level key pair in subset. In [5], the protocol is used for cluster based nodes only. These conventions are talking about giving security to decentralized systems. In WSNs, there is no such focal power to give this security. In [1], the creator talked about how elliptic bend cryptography utilized as a part of secure gathering correspondence. In [2], the portal part is chosen based on the most elevated force of hub. Be that as it may, picking the most elevated force node postures new issues in MANETs. In [7], the confirmed convention was planned utilizing the elliptic bend cryptography. Be that as it may, this is additionally helpless against a few assaults. Our plan to outline another security convention for sensor networks utilizing elliptic bend cryptography in view of different forms in elliptic curve.

The approaches to place secret keys on individual sensor nodes can be classified in two categories: key distribution and on-line key generation. In the first class, the keys are generated in a cryptographically secure manner by a central entity, such as the manufacturer of the sensor motes, and stored directly in the memory of the devices. Some protocols store only a random subset of all possible keys on each sensor mote and ensure the availability of shared keys probabilistically. The next step in the protocols range from a direct usage of the pre-distributed keys (e.g., in case of a planned node deployment), to probabilistic methods where neighboring nodes have to agree on common keys from a set of pre-distributed keys. As the sensor motes are not able to store the keys for every possible connection as the number of keys grows too fast, only a subset of the keys is stored, and the protocol only guarantee that sensor nodes can find common keys with a sufficiently high probability. These random schemes can limit the impact of node captures because in this case only a subset of keys is leaked. Alternatively, the keys can be distributed after deployment using secure physical connections, but this approach does not scale well with an increasing number of nodes.

The second class of key management protocols suits the needs of wireless sensor networks better: the on-line generation of secret keys after network deployment. As the topology is known locally to the network nodes at that time (the nodes can broadcast discovery messages to initiated contacts with the surrounding nodes), only the necessary keys must be generated. This promises to be a very efficient and scalable approach to wireless sensor network key management and is therefore explored further.

III. ELLIPTIC CURVE CRYPTOGRAPHY BASED ON GROUP THEORY

ECC [1-3] has turn into the cryptographic decision for specially appointed systems and specialized gadgets because of its size and proficiency advantages. Elliptic bend figure utilizes little keys also, is computationally exceptionally proficient, which makes it perfect for the littler, less effective gadgets being utilized today by greater part of people to get to network administrations. The elliptic bend crypto framework (ECCS) is a crypto-calculation strategy for using a discrete logarithm issue (DLP) over the focuses on an elliptic bend. Bunches which additionally obey commutative or symmetric property are known as Abelian gatherings. Abelian gatherings are broadly utilized as a part of cryptography, as the request of the sender-recipient transmission ought not to confound the regular key.

The abelian gathering of purposes of an elliptic bend, because of the littler key size (and subsequently lower number of individuals from the shut set), that is much littler in size, in the meantime keeps up the same level of security. Conclusion, a central property of gatherings, is utilized. The modulo (n) operations causes the area to have limited number of individuals. This guarantees the issue is reasonable for the substantial beneficiary, and in addition for the issue to be hard eg: discrete log (for Diffie-Hellman, or Elliptic Curves, and prime factorisation for RSA). We take note of that for a non-gathering say, y = xa, which is not constrained (not shut), in any case, over interminable genuine numbers, or whole numbers. It is simple for a gatecrasher after some time to guide, or theory, the exponential example, from the arbitrary specimens listened stealthily. On the off chance that we adjust this to y = xa mod(n), where a, x, y, n are whole numbers and x, and y values presently turns out to be more arbitrary, and henceforth it turns out to be much harder for an interloper to figure any example. In the meantime, given y, what's more, n, freely known values in broad daylight key cryptography, it turns out to be exceptionally hard to figure x. This is because of the hardness of the discrete log issue which is because of the gathering conclusion necessities.

The typical representation of an elliptic curve is y2 = x3+ax+b with a,b are integers. (x,y) are the points on x and y coordinates. We avoid curves where points (x,y), such that, x, and/or y is irrational, or transcendental. In cryptography, elliptic curves restricted over the domain of rational numbers (Q), is found to provide sufficient hardness in the discrete logarithm problem. For k to be an integer, we have to allow the coordinates of points (x,y) to be rational numbers. Thus points M, and P on the elliptic curves are allowed to take (x,y) values in rational numbers, such that M = kP where this operation is called scalar multiplication. The much smaller size keys, makes ECC very promising for the wireless, smaller size, smaller memory, bandwidth and power limited devices. 160 bit keys in elliptic curves provide same levels of security as 1024 bit RSA. Likewise 224 bit key in elliptic curve provide same levels of security as 2048 bit key in RSA.

IV. PROPOSED SCHEME

A. Motivation

In mobile ad-hoc networks, the security is main concern in achieving the efficient and deployable network for military and rescuer areas. In security, there are three mechanisms to be maintained: Confidentiality, Authentication and Non-repudiation. Confidentiality maintains that the particular message is to be received by the authorized receiver.

Authentication assures that the particular message is being sent by a authorized sender. Non-Repudiation assures that any sender or receiver could not able to deny the previous transactions (Sender cannot deny that the previous message had not been sent by me or receiver cannot deny that the previous message had been received by me). If any security algorithm provides these three security mechanisms, it will be a good and deployable security algorithm. But providing these mechanisms in ad-hoc networks is difficult since there are no such infrastructures. All these mechanisms need a central authority to store the key pairs of the mobile nodes. For example, in an military environment any one mobile node can be selected as a central node to which all other mobile nodes send their key pairs. In these networks, the nodes other than an central node have limited power and low stability.

B. System Model

In the proposed system they are used Elliptic Curve Diffie-Hellman Cryptography for group key generation. In our proposed system we are using three elliptic curve forms to analyze which curve is better for secure gathering key generation with respect to time and energy consumption. The gathering key can be calculated by using the formulae [3]

$K_g = Pf_{id}(R_n, G_k)$.

Where Pf_{id} = Polynomial Function,

R_n = Random number,

And G_k = Group key generator.

The polynomial function may be one of the three elliptic curve forms. The equations of the three elliptic curve forms are namely,

i) Weierstrass curve $y^2 = x^3+ax+b$,

ii) Edward curve $x^2+y^2 = c^2(1+dx^2y^2)$,

And iii) Jacobian curve $y^2 = x^4+2ax^2+1$.

V. EXPERIMENT AND RESULTS

We use the help of Network Simulator Version-2 (NS2) to simulate our proposed model. We have successfully implemented secure knowledge algorithm to secure AODV routing protocol against black hole attack using NS- 2.35.

We analyze that Edward curve is the best curve with respect to time taken to generate gathering key and remaining energy present in the nodes after key generation. The key generation may be centralized or distributed. In this paper we also analyze the gathering key generation both in centralized and distributed with respect to response time, remaining energy and routing overhead.

A. Comparison of Energy

In our analysis the best form of the Elliptic curve is selected on the basis of the energy consumption during the key generation.

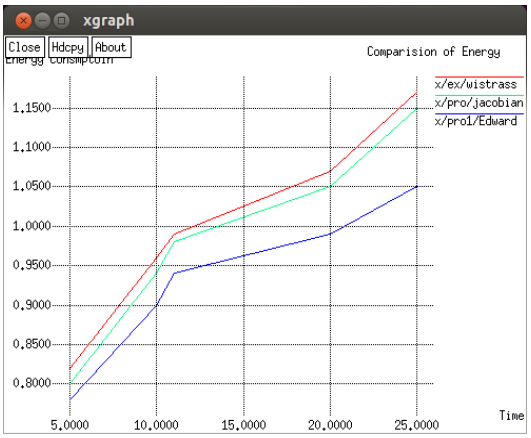

Figure 1: Comparison of Energy

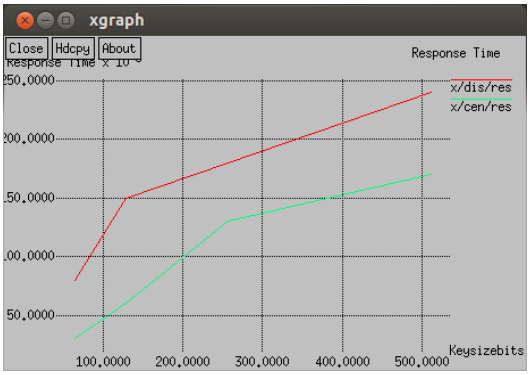

Figure 2: Response Time

Figure 3: Remaining Energy

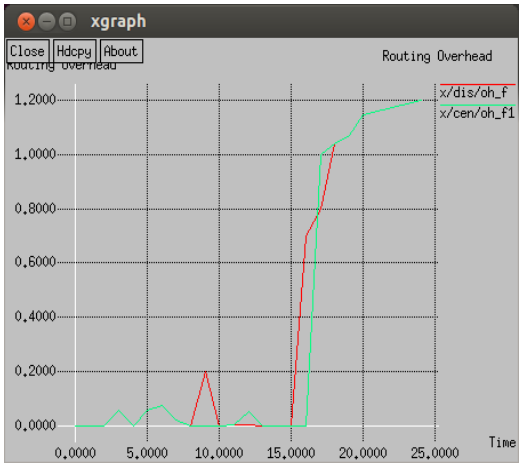

Figure 4: Routing Overhead.

VI. CONCLUSION

Our Analysis shows that Edward curve is the best form for gathering key generation in sensor networks. It gives equal security even the key size is low. Response time and energy consumption is better in centralized group key generation. But in routing overhead it alters to both centralized and distributed. In elliptic curve we have many forms. We can extend this analysis for remaining curve forms to get better security.

REFERENCES

[1] K.Muthumayil, Dr. V. Rajamani, Dr. S. Manikandan, M. Buvana, "*A Group Key Agreement Protocol based on stability and power using Elliptic curve cryptography*," IEEE International Conference on Communication, 2011, pp 1051-1056.

[2] Hsiao-hing Lin, Ming-Kung Sun, Hui- Tang Lin, Wen-Chung Kuo, "*Multi-level and Group-based Key Management for Mobile Ad Hoc Networks*", IEEE,2012, pp164-167.

[3] N. Suganthy, V. Sumathy," *Energy Efficient Key Management Scheme for Wireless Sensor Networks, CCC publications"*, 2014, pp 71-78.

[4] Kavitha Ammayappan 1, 3, Ashutosh Saxena 2 and Atul Negi , "*Mutual Authentication and Key Agreement based on Elliptic Curve Cryptography for GSM*", IEEE 2006 pp 183-186.

[5] Haimabati Dey, Raja Datta, "*Transmission-Efficient Group-key Generation in Large Dynamic MANET Environments*", 2012 Third International Conference on Emerging Applications of Information Technology(EAIT), IEEE 2012 pp355- 360.

[6] Hai-Ying, Zhou, Dan-Yan Luo, Yan Gao, De-Cheng Zuo, "*Modeling of Node Energy Consumption for Wireless Sensor Networks*" , Scientific Research, 2011, pp 18-23.

[7] Ms.P.G.Rajeswari, Dr.K.Thilagavathi, "*An Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Mobile Networks*", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.2, February 2009 pp 176-185.

[8] Nils Gura, Sheueling Chang Shantz, Hans Eberle, Sumit Gupta, Vipul Gupta, Daniel Finchelstein, Edouard Goupy, and Douglas Stebila , "*An End-to-End Systems Approach to Elliptic Curve Cryptography*" Springer-Verlag Berlin Heidelberg 2003 pp 349-365

[9] K. Kaabneh and H. Al-Bdour, "Key Exchange Protocol in Elliptic Curve Cryptography with No Public Point", American Journal of Applied Sciences 2 (8): 1232-1235, 2005

[10] Krishnan Kumar, J. Nafeesa Begum, V. Sumathy, "A Novel Approach towards Cost Effective Region-Based Group Key Agreement Protocol for Ad Hoc Networks Using Elliptic Curve Cryptography", Int. Communications, Network and System Sciences, 2010, 3, 369-379

[11] V. Vijayalakshmi and T.G. Palanivelu, "Secure Antnet Routing Algorithm for Scalable Adhoc Networks Using Elliptic Curve Cryptography", Journal of Computer Science 3 (12): 939-943, 2007.

[12] Key-agreement protocol - Wikipedia, the free encyclopedia.html

