Secure Key Generation and Transmission Protocol in Wireless Sensor Networks

Ch.BhogeswaraRao[1], Ramesh Yegireddi[2],G.S.Pavan Kumar[3]
M.Tech Student[1], Associate Professor[2], Assistant Professor[3]
[1,2,3]Department of CSE, Aditya Institute of Tech. & Management (AITAM) Tekkali,Andhra Pradesh, India[1]

Abstract: *We propose a dynamic and recursive group key generation protocol in wireless sensor networks with efficient authentication mechanism with block based signature. Key generation protocol is dynamic because key can be updated when a new member added to group list and key can be updated when user eviction. Block based signature mechanism applies signatures over individual blocks for authentication and cryptographic implementation maintains the data confidentiality.Our proposed result gives more efficient results than traditional approaches.*

I. INTRODUCTION

A certificateless-successful key administration convention for secure correspondence in element WSNs characterized by hub portability. The certificateless-successful key administration supports productive key upgrades when a hub leaves or joins a cluster and guarantees forward and in reverse key mystery. The convention additionally supports productive key revocation for compromised hubs and minimizes the effect of a hub trade off on the security of other correspondence joins. A security examination of our plan demonstrates that our convention is compelling in shielding against different attacks. We implement certificate less-successful key administration in Contiki OS and recreate it utilizing Cooja test system to survey now is the right time, vitality, correspondence, and memory performance[1][2].

Dynamic wireless sensor systems (WSNs), which enable versatility of sensor hubs, encourage more extensive system scope and more accurate administration than static WSNs. Accordingly, dynamic WSNs are in effect quickly adopted in observing applications, for example, target following in front line observation, human services frameworks, movement stream and vehicle status checking, dairy cows wellbeing checking[3]. Be that as it may, sensor gadgets are vulnerable to vindictive assaults, for example, mimic, interference, catch or physical obliteration, because of their unattended agent situations and slips of network in remote correspondence. In this way, security is a standout amongst the most imperative issues in numerous critical element WSN applications. Dynamic WSNs along these lines need to address key security necessities, for example, hub authentication, information, classification and uprightness, at whatever point and wherever the hubs move.

In certificate less open key cryptography (CL-PKC), the client's full private key is a combination of an incomplete private key created by a key era focus (KGC) and the client's own mystery esteem. The extraordinary organization of the full private/open key pair evacuates the requirement for authentications furthermore resolves the key escrow issue by expelling the responsibility for the client's full private key. We likewise take the advantage of ECC keys characterized on an added substance bunch with a 160-bit length as secure as the RSA keys with 1024-bit length [4].

Wireless sensor systems can permanently screen, control and react to occasions and marvels in a predefined situation by various sensor gadgets. Be that as it may, these sensor hubs have perceptible limitations on vitality, computation and transfer speed assets. Aside from these restrictions, WSNs have one of a kind attributes, for example, SN versatility, huge adaptability, constrained assets, extraordinary movement patterns and questionable responses to numerous sorts of assaults. The structure of WSNs can be partitioned into two general classes: homogeneous and heterogeneous. All SNs are like each other and, on account of homogeneous WSNs, are conveyed in a level engineering. This level design limits system scalability and performance contrasted and heterogeneous WSNs[5].

The key administration conventions are arranged in light of encryption strategies into three classes. Symmetric schemes, likewise called pre-dispersion schemes, are responsible for stacking some keys in the SNs preceding the deployment stage, taking into account either their physical or remote interfaces. Asymmetric models are more adaptable however extremely heavyweight in sensor systems. The late advance in ECC and IBC opens new chances to apply open key cryptography in WSNs[6].

II. RELATED WORK

So many previous key generation models evolved in years of research, every approach has its own advantages and disadvantages. In Key generation model nodes usually depends of third party key generation center ,it may be a security if

we completely rely on KGC and key should be updated dynamically so we need to update KGC periodically, so it is a time consuming process. Authentication is major loss while identification of data packets from genuine users .The main disadvantages with traditional models are Centralized architecture generates static keys per session and completely rely on third party key generation center and Data may be decoded even though authentication failed.

The conventional cryptographic methods are impractical in Wireless Sensor Networks as a result of related high vitality and computational overheads. This calculation supports the foundation of three sorts of keys for every sensor hub, an individual key imparted to the base station, a couple astute key imparted to neighbor sensor hub, and a gathering key that is shared by every one of the hubs in the system. The calculation utilized for establishing and upgrading these keys are vitality proficient and minimizes the contribution of the base station. Polynomial capacity is utilized as a part of the study to figure the keys amid instatement, enrollment change and key trade off. Intermittently the key will be updated [7][8].

To overcome the issue of vitality insufficiency and memory stockpiling and to give satisfactory security, the vitality proficient plan is proposed. It functions admirably in indistinct organization environment. Unapproved hubs ought not be permitted to establish correspondence with system hubs. This plan when compared with other existing plans has a low overhead in calculation, correspondence and capacity [9].

The small sensor hubs, which comprise of detecting, information processing and imparting segments, leverage the possibility of sensor systems taking into account the cooperative exertion of countless. Sensor hubs are sent in unfriendly situations or over expansive topographical range. The hubs could either have a settled area or could be randomly conveyed to screen the earth. The hubs then sense natural changes and report them to different hubs over adaptable system engineering. They have along these lines discovered application areas in front line correspondence, country security, contamination detecting and activity observing. The restricted variables of utilizing sensor hubs are that they have constrained battery power and less memory limit[10].

To control data access in a sensor domain just approved hub must know the way to disseminate the data that is obscure to the traded off hubs. The correspondence keys might be pair savvy, or gathering astute. These keys to be overhauled to keep up security and resilience to assaults. A portion of the proposed work depended on static plans and some are on element plans. Despite the fact that numerous conventions have been intended with the end goal of security in sensor environment, lamentably, hub bargaining is seldom or insufficient investigated and the greater part of these conventions have a powerless resilience to assault.

III.PROPOSED WORK

We are proposing an empirical model of efficient key generation protocol with dynamic key generation while member addition and eviction. We are generating a multi cast key mechanism with recursive chebyshevrules recursively and dynamically. Initially data component can be divided into blocks and applies signature over blocks with Signature based mechanism and forward to the destination node and also verifies authentication at receiver end.The main advantages o the proposed work are , In decentralized architecture ,user need not depends on KGC and Key generation is recursive and dynamic for member addition and eviction and Authentication can be maintained with block signature algorithm

Sender segments the total data block and applies signature over individual blocks in bit level with block signature algorithm and attaches the sender id and receiver id, data packets authentication can be verified at receiver with same block segmentation and signature verification, it verifies the authentication as well as identifies block which are corrupted over network.

Block signature algorithm:

Algorithm: Generate file with integrated Signatures

Input: User File in ASCII (Fo)

Output: File with Signature appended at end of (Fn)

Method: For apply hash function on each n byte block of file which is corrupted? If we consider it with the file we perform the following steps to make (m mod n)= 0 of Fo

M← Calculate Length of (F0)

n← Length of Block (any one of128/ 256 /512/ 1024 /204/4096/ 8192) bytes

res← reserved 16 bytes

P ←m mod n

Q ← n- (P + res)

if(Q > 0)

F←Append Q zeros at the end of F_0

Else if(Q < 0)

R ←n+ Q

F1 ←Append R zeros at the end of F_0

F1← Append res at the end of F_0

In order to generate Signatures of Fl, perform the following steps

I← Calculate_ Length of (F_l)

count←l/n

For j←1 to count

S ← 0

S ←reverse[$\sum^{n}_{A=1}$((A XOR B) v (A ∩ B))]

Where B <- to_Integer (to_Char (A))
Sig ← Sig+ to-Binary (S)

Fn←F1 + Sig

Key Generation:
In our proposed work contains a system for gathering key management and productive correspondence cost in correspondence. It contains a calculation for creating keys for part removal and expansion from a gathering. This methodology is purported as rekeying. From secure key era we embrace chebyshev map cycle idea. It is utilized for creating positive keys for clients. There is an impediment in past methodology, for example, the premise of the above calculation is semi-bunch property, which is constantly valid for Chebyshev delineate. On the other hand, we must perceive that, on one hand, Chebyshev guide is characterized over genuine numbers and delicate to introductory conditions
Chebyshev Recursive Algorithm:
F0(x) = 1 mod N
F1(x) = x mod N
$Fn(x) = 2xFn\text{-}1(x) – Fn\text{-}2(x)$ mod N
Where x is users secret key
The Algorithm is as follows:
There are some notations such as 'n' is number of members in the group. 'x' is public key for user. 'N' is large prime number.
(1) The first member calculatesF_1 (x) and sends it to thesecond member.
(2) The second member calculatesF_2 (x) and sends it tothe third one.
(3) Repeat thisuntil the last member calculatesF_{rn}(x) and sendsit to the first member.

(1) The first member calculatesFn1 (Frn(x)) and sends it tothe second member.
(2) The second member calculates F_2 (F_1 (x)) and sends itto the next.
(3) Repeat this until the last member calculatesF_{rn}(F_{rn-1} (x))and sends it to the first member.
Stage i.
(1) The first member calculatesF_1 (F_{rn}(· · · $F_{rn\text{-}i+2}$(x)))and sends it to the second member.
(2) The second member calculatesFn2 (Fn1 (· · · Fr_{n-i+3}(x)))
and sends it to the next.
(3) Repeat this until the last member calculates F_n(F_{n-1} (⋯ F_{n-i+1}(x))) and sends it to the first member.
By n − 1 stages message exchange by any memberand the
with member calculates the group session key by:
F_i (F_{i-1} (· · · F_1(F_n(F_{n-1}(· · · F_{i+1}(x)))))) which is equal to

$F12\ldots rn$(x)

Data encoding or decoding i.e data confidentiality can be maintained by the cryptographic implementation in terms of coefficient and reminder vectors. This algorithm uses a finite alphabet set, constant value Δ for encryption and a decryption of the message and is used as a secret key. This Δ is generated using Diffie-Hellman key generation algorithm to provide more security to algorithm. The sender generates Remainders and Quotients using Δ value and the compression performs only on the Quotient vector further these two values forwarded to the receiver to ensure the confidentiality of the message. The receiver decompresses and decodes the message using compressed quotient and remainder vector.

- MOD-ENCODER Encoding Algorithm:
  - Input : M ∈∑, Δ value
  - N=|M|, i.e length of M
  - Z=n * bit size, i.e bit size is the number of bits require to represent each character
  - For i=1 to n

Read m_i the i^{th}character from M
Find RR[I]=I(m_i)%Δ
Find QQ[I]=I(mi)/Δ

- Representation of R
  - For I=1 to n
  - Represent R[I] in base Δ
- Representation of Q

- MOD-ENCODER Decoding Algorithm:
  - Input : Bi-tuple <R,Q>, Δ value
  - Convert Q from Base 10 to Base B
  - Let QB=(q1,q2,….qn) be the representation in Base B
  - Interpret R as a vector of Base Δ number
  - For 1 ≤ i ≤n
  - I=qi × Δ + ri

Where qi the ith digit of QB,ri the ith element of R.

- Mi=I-1(i)
- M=(m1,m2,….mn)

The encoded message is a bi-tuple of which, the first is a vector of quotients denoted as Qand the second is a representation of remainders denoted as Rwith respect to a modulus M. The secrecy of the message is retained by communicating Rover a secure channel using some standard encryption mechanism. The computation overhead is also reduced as the encryption is done only on one half of the encoded message.

IV. CONCLUSION

We have been concluding our current research work with efficient and secure key generation protocol for generation of secure key. Data confidentiality can be maintained by the Cryptographic model and Data integrity can be maintained by the signature algorithm implementation.This block signature algorithm maintains the integrity with minimal time, our proposed results gives optimal results with less time and space complexity.

REFERENCES

1 Simpli´cio, M.A. Jr., Barreto, P.S.L.M., Margi, C.B., Carvalho,T.C.M.B.: 'A survey on key management mechanisms for distributedwireless sensor networks', Comput. Netw. J., 2010, 54, (15),pp. 2591–2612

2 Zhang, J., Varadharajan, V.: 'Wireless sensor network key managementsurvey and taxonomy', J. Netw. Comput. Appl., 2010, 33, pp. 63–75

3 Samundiswary, P., Priyadarshini, P., Dananjayan, P.: 'Performanceevaluation of heterogeneous sensor networks'. IEEE Int. Conf. onFuture Computer and Communication, 2009, pp. 264–267

[4] Eltoweissy,M.; Moharrum,M.; Mukkamala,R.; Dynamic key management in sensor networks,
IEEE Communications Magazine, 44(4):122- 130, 2006.

[5] Du,W.; Deng,J.; Han,Y.S.; Varshney,P.K.; Katz,J.; Khalili,A.; A pairwise key predistributionscheme for wireless sensor networks, ACM Trans. on Information and System Security,8(2):228-258, 2005.

[6] Jen Yan Huang; I-En Liao; Hao-Wen Tang; A Forward Authentication Key ManagementScheme for Heterogeneous Sensor Networks, EURASIP J. on Wireless Communications andNetworking, Article ID 296704, DOI:10.1155/2011/296704, 2011.

[7] Eschenauer,L.; Gligor,V.D.(2002); A key-management scheme for distributed sensor networks,Proc. of the 9th ACM Conference on Computer and Communications Security, Washington,DC, USA, 41-47, 2002.

[8] Chan,H.; Perrig,A.; Song, D.; Randomkeypredistribution schemes for sensor networks, Proc.of IEEE Symposium on Security And Privacy, 197-213, 2003.

[9] Liu,D.; Ning, P.; Establishing pairwise keys in distributed sensor networks,Proc. of the 10th ACM Conference on Computer and Communications Security (CCS 03), Washington, DC,USA, 52-61, 2003.

[10] Sencun Zhu; SanjeevSetia; SushilJajodia (2003); LEAP: Efficient Security Mechanisms forLarge Scale Distributed Sensor Networks, Proc. of the 10th ACM Conference on Computerand Communications Security, pp.62-72.