Improved Authentication and Integrity Verification in Wireless Sensor Networks

S.Sadakvalli
Mtech(CSE)
Gudlavalleru Engineering college

Ch.Suresh.babu
Associate professor
Dept of CSE
Gudlavalleru Engineering college

Abstract –

In an unprotected environment of Wireless Sensor Network, the authentication scheme for multicast secure communication has to be designed with limited usage of resources and computation. Wireless Sensor Network are diversified, several new issues such as mobility of sensor node are raised and bring security issues such as re-authentication and tracing the node movement. In the dynamic sensor network, mobile sensor nodes will continuously move around and frequently reconnect to other sensor nodes. While many security protocols to such networks occur significantly large overheads because their design only considered the static networks. Sensor nodes employ wireless communication in order to exchange data with their peers. Cryptography plays an important role in securing networked computer systems. It provides the basic functionality for protecting the confidentiality, integrity, and authenticity of messages and data. Adding a message authentication code (MAC) to such a small sensor message adds a significant In this proposed work, we show our design for the efficient node authentication and key exchange that reduces the overhead in node re-authentication and also provides untraceablity of mobile nodes. We introduce protocols that are improved MD5 hashing approach with key crypto system based and public key crypto system. Efficient method of membership verification for re-authentication of mobile node and show the performance analysis of our membership verification. Using this method, we propose an efficient and scalable reauthentication protocol over wireless sensor network. Also, we provide performance and security analysis of our protocol.

Keywords –Network,Client,Server,Nodes.

I. INTRODUCTION

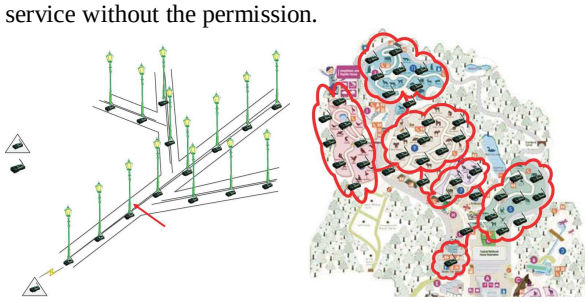
Wireless Sensor Network (WSN) is the network that consists of lightweight devices with short-ranged wireless communication and battery-powered. The devices have the sensor that gathers the environmental information and etc. After sensing this information, the devices send the information to the networks. We define such devices as sensor node, and the core parts of the network as sinks and the base station. Authentication is undoubtedly an expression that is used, maybe even abused, inside a very broad sense. By any means, it aims to insure that any entity is who it appear to be or that information has never been altered by unauthorized parties before reaching the recipient. Both terms must be satisfied to obtain message authentication with which we deal in this work. Message authentication demands than a party B receiving a message is assured of the identity of a given party A which originated text [1]. This also includes information integrity, i.e. the peace of mind that the message haven t been manipulated, as with case of a spoofed message A would seldomly are the originator of this very message.

In this particular work we conceive authentication as message authentication. Should we solely address the challenge of assuring a celebration of another's identity, we work with the term source authentication. Authentication in wireless sensor networks (WSN) is a challenging problem. Some well known mechanisms to unravel authentication generally typically are not applicable as they simply require costly computations that's incompatible onto the restricted capabilities of a sensor in regards to computation power. Several works inside the literature addressed the challenge affordable authentication and presented procedures that are solely in accordance to power-saving operations.

These solutions work fine under specific constraints but have some significant drawbacks if the application does not meet these constraints. This work discusses the brain teaser of low-cost authentication for Wireless Sensor Networks. A protocol is presented that, depending on the structure of the WSN and dependent upon the requirements defined by the applying, presents an efficient solution. We distinguish and discuss this problem for three various kinds of WSN: (a) a little WSN that supports just one service, (b) a limited WSN that supports several services and (c) large WSNs that, additionally, are able to address specific regions of the whole of the network. The initial two, (a) and (b), are conceivable for various services that improve our lifestyle. The security grade of driving, just for instance, would increase should a vehicle gets informed on the status of the street in front of critical areas as bridges.

Contrariwise, french scenario (c) aims at monitoring larger areas as, for instance, forests to detect fire or to observe wildlife animals' movement[2].

Based on these observations, the authentication protocol for wireless sensor network should support the following security requirements. Mutual authentication: an end-user and sensor node is necessary to recognize if the communicating party is basically a legitimate entity or possibly not. Anonymity and accountability: Since an end-user having his/her own mobile node would like to preserve the financial information (i.e., identify, service usage, and etc) during accessing the wireless sensor network. Although anonymity can protect the privacy in an end-user, it can help a malicious user access the service without the permission.



Differentiated control access: Although a professional would like to provide differentiated services in accordance to access privilege of his/her subscribers, anonymous communication through an authentication server allows the server to gain access to the subscription information of this very professional that needs to be protected.

Resilience against node compromise: Following the sensor nodes are deployed in a target area, anyone can hang around within the sensor network. Consequently, the sensor node inside the network can be compromised. That's why re-authentication really should be resilience against node compromise.

Scalability: Like the number of re-authentication requests in wireless sensor network might be same as the volume of citizens inside a city, the re-authentication protocol may need to consider scalability issue to insure that the wireless sensor network are able to do its own functionality and at the same time provide reauthentication towards the end-user.

Lightweightness: Since the sensor node provides the limited resources, re-authentication protocol should really be lightweight seen from the view of computation and communication cost[1].

II. LITERATURE SURVEY

LEAP (Localized Encryption and Authentication Protocol) Is a representative scheme of master key based approach [1]. By using the shared master key and identifiers of its neighbors, each sensor node generates pairwise keys with its neighbors. In relation to random key pre-distribution approach, LEAP provides fully connected network topology with less storage requirements, about 4K bytes when 256-bit key's used. After generating all pairwise keys, each sensor node should erase the shared master key. But, the challenge within this approach is the fact that the adversary can obtain the master key before erasing and generate all pairwise keys among the entire network. In 2005, Hartung et al. showed that anyone can get all data within 1 minute using chip-debugging procedure.

Typical example of trusted party based approach is HIKES (HIerarchical Key Establishment Scheme) [3]. In 2007, Ibriq *et al.* proposed HIKES to provide robustness against well-known routing attacks while supporting the authentication and key distribution efficiently. Compared to the above two schemes [1], , HIKES needs less storage, about 3K bytes when 256-bit key is used, and enhances resiliency against node compromise. Also, as the network size increases from 1000 to 9000, according to the simulation result in [3], the energy consumption of a cluster head on key management is 3% to 20% while the cluster head in LEACH-type scheme dissipates 13% to 82% energy on key management. That's why we believe that trusted party based approach is more suitable than the other approaches. However, the adversary can reuse the stored key escrow table to guess pairwise keys of neighbors of the compromised node. Also, the adversary gets identifiers of sensor nodes. Still, HIKES requires a large amount of communications for authenticating cluster members, although it aggregates authentication message at the cluster heads. Han *et al.* proposed an efficient re-authentication method [4] . As the node authentication is done by the base station, the scheme is one of example of the trusted third party based approaches. However, the cluster head should directly communicate with the nearby cluster head to share a pairwise key and update the key for supporting re-authentication of the mobile node. As the number of the nearby cluster head increases, the communication cost will increase[1].

Perrig, Canetti et al. proposed the often quoted low cost TESLA authentication protocol [2]. TESLA solely uses one MAC attached to each packet which is generated by using continuously new keys which are published at a later point in time. On receipt of such a message, a recipient stores the packet, waits for the revealment of the key and checks its validity. If this verification fails, the packet is discarded. To prevent an adversary from using its own keys, each key belongs to a specific *hash chain* generated by the sender . Initially, each receiver obtains the last value of the chain and can therefore infer the validity of the key.

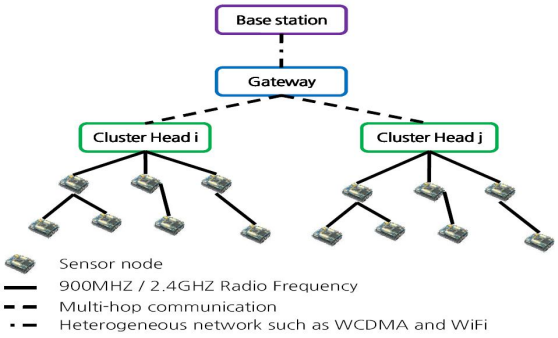
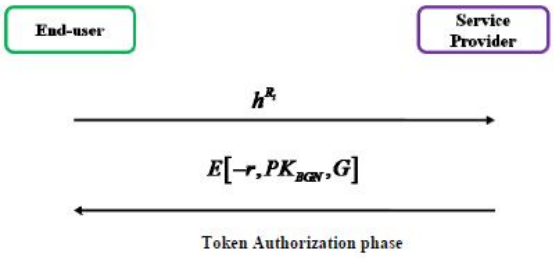


Figure shows our system model in [1]. In this model, the sensor network consists of a base station, several gateways, multiple cluster heads and many sensor nodes. A sensor node, having a battery power, gathers the nearby interesting event (*i.e.*, environmental information, location information for indoor location supporting application, and living human in disaster area) and sends the information to a cluster head. Then, the cluster head aggregates the received information and forwards it to the base station via a gateway. Since the sensor nodes in the same cluster report very similar data compared with other nodes in the different cluster, data aggregation technique is required to extend the lifetime of the sensor network.

MEMBERSHIP VERIFICATION AND ITS ANALYSIS

Token authorization phase



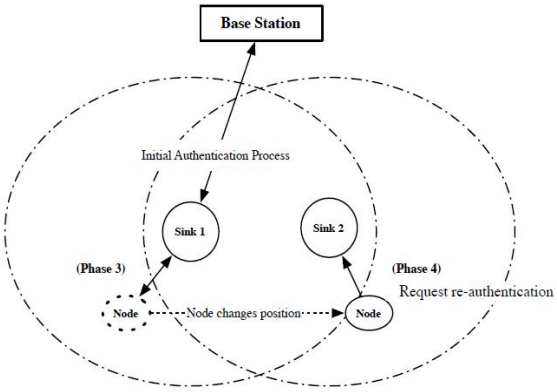
Entity registration phase

After token authorization phase, the end-user should register him/her with the base station in order to obtain nonce RBS. The base station verifies whether the end-user is a legitimate subscriber of the target service through membership verification. Only if the verification result is true, the base station sends RBS to the end-user.

Entity authentication phase

In the entity authentication phase, the end-user having the mobile node and cluster head establish KU,CH=H(RBS+1||RU). Using this key, the communication between the end-user and cluster head can be secure. Since RBS is only known to the cluster head and end-user, they can share a secret key KU,CH. We employ HMAC in order to support message integrity.

III.PROPOSED SYSTEM



Node is initially authenticated by Sink 1 (Phase 3), and requests re-authentication to Sink 2.

Thus our model consists of following five phases.

- **Phase 0** The common neighbor discovery
- **Phase 1** Setting up neighbor sink relationship
- **Phase 2** Neighbor group authentication key share.
- **Phase 3** Initial node authentication
- **Phase 4** Node re-authentication
- Message Integrity Verification Using **Improved MD5**.

Improved RSA algorithm:

Seeing from key management, RSA algorithm is more superior to the DES algorithm. Because the RSA algorithm can distribute encryption key openly, it is also very easy to update the encryption keys, and for the different communication objects, just keep the decryption keys secret; DES algorithm requires to distribute a secret key before communication, replacement of key is more difficulty, different communication objects, DES need to generate and keep a different key.

Key generation:

1. Choose two prime numbers p and q.

2. Calculate n = p × q.

3. Calculate Φ(n) =Φ (p × q) = (p-1)(q-1).

4. Select one e, which satisfies gcd(Φ(n), e) = 1. 1 < e <Φ(n).

5. As ed = 1 mod Φ(n), utilize Euclid's Algorithm to get d=e-1

mod Φ(n).

6. A pair of public keys is obtained, which is {e, n}.

7. A pair of secret keys is obtained, which is {d, n}.

function ModExp(M, e, n) { n is odd }

Step 1. Compute n'.

Step 2. Mm := M · r mod n

Step 3. xm := 1 · r mod n

Step 4. for i = k – 1 down to 0 do

Step 5. xm := XOR(xm, xm)

Step 6. if ei = 1 then xm := XOR(Mm, xm)

Step 7. x := XOR(xm, 1)

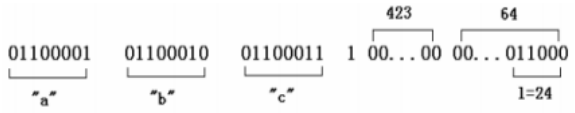
Step 8. return x

In steps 2 and 3 valueM and 1 are converted to Montgomery's domain, while exponentiation is done in steps 4-6. In step 7, result is converted back from Montgomery's domain and encrypted data are obtained. Function MonPro should implement a Montgomery reduction (also known as Montgomery multiplication) and has a central role in the modular exponentiation.

One Improved Hash Algorithm

Although we have extended this hash algorithm to 160-bit, it is primarily based on MD5, only introducing one excellent assistant function from 160-bit SHA1. So far, we name it MD5plus algorithm temporarily.

The data filling of MD5plus works almost as the same as MD5 and SHA1. See figure.



We have to append ox80 to low-bit of the handling information (actually, it equals appending some "0" after adding a "1" to the information). Supply the information with "0" until length mod 512 equals to 448. At last, append information length in the end (most hash algorithms use this method to fill data length).

1. Generation of parameter

Step1: Generate Message digest for M using SHA 256
Step2: Declare key length L,N where
512<=L<=1024
512<=N<=1024
Step3:Declare the variables p,q,g

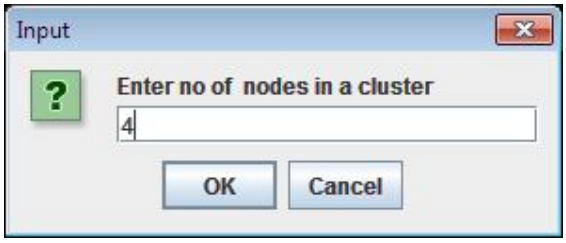
2. Signing or creation of signature

Step1:Declare random integer k,0<k<q
Step2: Generate Signature s,r
Step3:if(s=0)
Use different k value
else
$r = (g_k \bmod p) \bmod q$

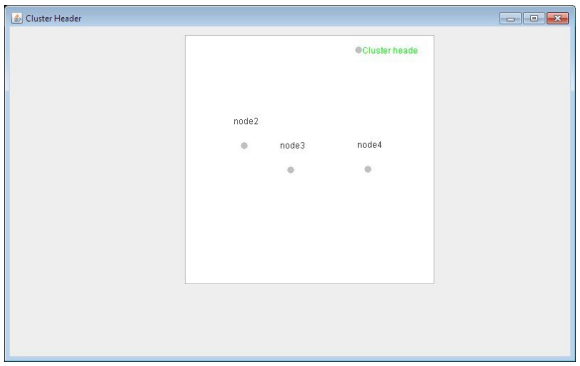
3. Verifying

Step1: Declare verifying function v,
Step2: Declare variables u1,u2,w
Step3:Generate w, $w = s_{-1} \bmod q$
Step4:Generate u1,u1 = H(m)·wmodq
Step5:Generate u2,u2=r.w mod q.
Step 6:Generate Verifying Function V,
$v = ((g_{u1} \cdot y_{u2}) \bmod p) \bmod q$.
Step7:if(Verifying Function=Signature)
Valid Signature.
else
Reject.

IV. RESULTS



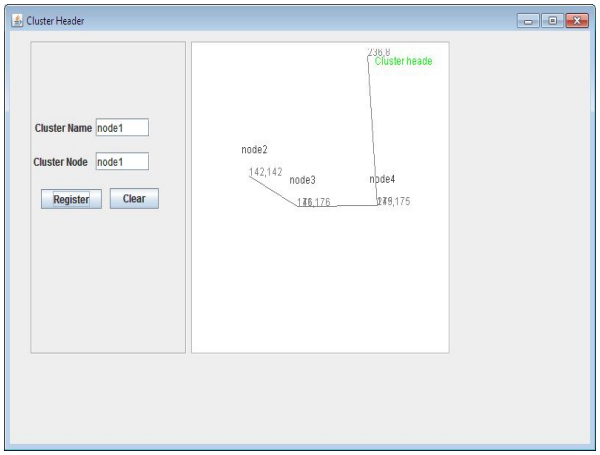
Enter number of sensor nodes



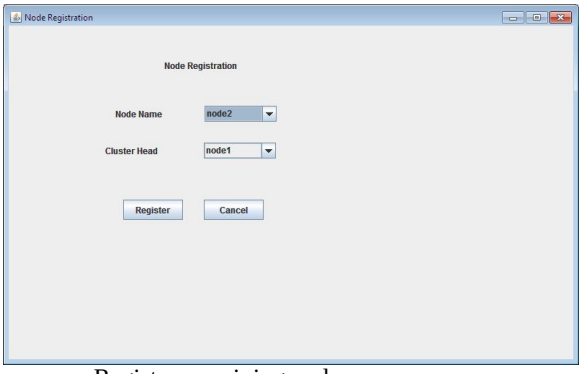
Sensor network is created with the specified nodes

Register head node of the network

Generate secured password for cluster head

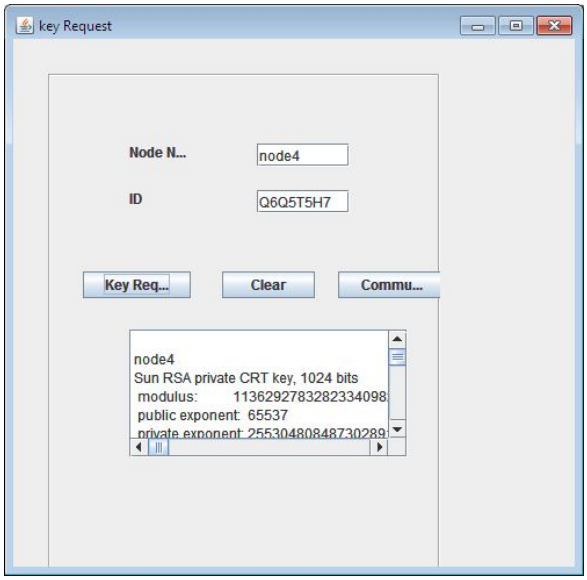


Sensor network construction after registration

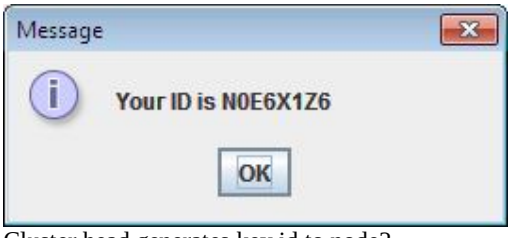


Register remaining nodes

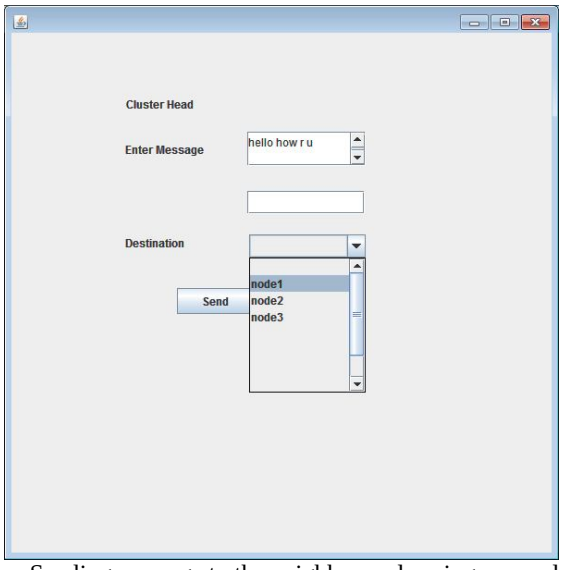
Node 2 registration request to cluster head



Key request from the node in the network

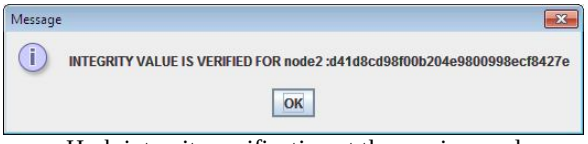


Cluster head generates key id to node2



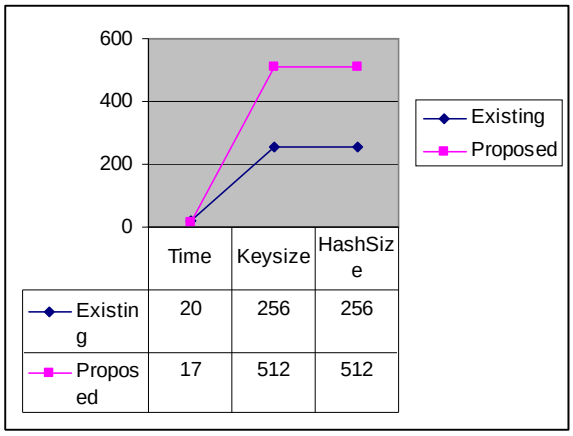
Sending message to the neighbor node using secured

mechanism



Hash integrity verification at the receiver end

Message received status



Comparative study between existing and proposed in terms of keysize hashsize and time.

V. CONCLUSION AND FUTURE SCOPE

By using Improved approach , re-authentication of wireless node is achieved, which provides Authentication, Intergrity, Confidentiality. Also it is not feasible for an opponent to find recover random integer from signing and verifying. Also, here, re-authentication protocol is used for membership verification and re-authentication of mobile nodes. Based on this method, an efficient and scalable re-authentication protocol over wireless sensor network is described. This protocol reduces communication overhead while increasing computational cost. The number of inspections is decreased when binning technique is used and increased when non-binning technique is used.

REFERENCES

[1]. An Efficient and Scalable Re-authentication Protocol over Wireless Sensor Network, Jangseong Kim, Joonsang Baek IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, May 2011.
[2]. Authentication and Information Integrity in Wireless Sensor Networks Diploma Thesis by Moritz Killat.
[3]. J. Ibriq and I. Mahgoub, “A Hierarchical Key Management Scheme for Wireless Sensor Networks”, 21st International Conference on Advanced Networking and Applications (AINA 2007), May 21-23, 2007, Niagara Falls, Canada, pp.210~219.
[4]Authentication in Smart Home and WPAN”, IEEE Trans. On Consumer Electronics, Vol. 56, No. 2, May 2010, pp. 591-596..
[5] L. Eschenauer and V.D. Gligor. A key management scheme for distributed sensor networks". In Proceedings of the 9th ACM conference on Computer and Communications Security (CCS). Washington. DC. USA, :41-47, 2002.

[6] Yun Zhou,“MABS: Multicast Authentication based on Batch Signature,” IEEE Transactions on Mobile Computing, Vol. 9, No. 7, pp. 982-993, Jul 2010.
[7] Dexin Yang and Bo Yang,“A Novel Two-Server Password Authentication Scheme with Provable Security,” IEEE International Conference on Computer and Information Technology (CIT), Bradford, UK, Jul 1, pp. 1605-1609, 2010.
[8] Kui Ren,“Multi-User Broadcast Authentication in Wireless Sensor Networks,” IEEE Transactions on Vehicular Technology, Vol. 58, No. 8, pp. 4554-4564, Oct 2009.
[9] Xuefei Cao,“Identity-Based Anonymous Remote Authentication for Value-Added Services in Mobile Networks,” IEEE Transactions on Vehicular Technology, Vol. 58, No. 7, pp.3508-3517, Sep 2009.
[10]. T. M. Baduge, A. Hiromori, H. Yamaguchi, and T. Higashino, “A distributed algorithm for constructing minimum delay spanning trees under bandwidth constraints on overlay networks,” Systems and Computers in Japan, vol. 37, no. 14, pp. 15–24, 2006.