An Integrated Approach for Anchor-Based Localization and Energy Efficient Secure Communication in WSNs

G.Soujanya
Computer Science Engineering
UCEK, Kakinada
Andhra Pradesh, India
e-mail:soujanya.guntuku@gmail.com

E.Suneetha,Assistant professor
Computer Science Engineering
UCEK, Kakinada
Andhra Pradesh, India
e-mail:suneethaeluri9@gmail.com

Abstract— In wireless environment the sensor nodes are more vulnerable to attacks due to openness of the network. Spoofing is a serious vulnerability of sensor nodes that can cause adverse effects. The proposed method includes Improved Attack Detection and Localization Scheme (IADLS) for spoofing attack detection and determining the position of an attack. And secure communication can be attained by using chaos based encryption. In this IADLS scheme, for detecting the attack pseudo identity can be used instead of IP address. SeRLoc (Secure Range-independent Localization) is a range-free algorithm which is unique in its secure design and can be implemented under low cost. To address the problem with SeRLoc, a special network design is required that covers all the sensor nodes in the network and assures location accuracy. To provide confidentiality a simple and fast RFCA (Robust and Fast Chaotic encryption Algorithm) mechanism is used where cryptanalysis is more difficult as it looks complex. Hence the solution for identity-based attacks is achieved, which assures accurate attack location and provides energy-efficient secure communication among authenticated nodes in the wireless sensor networks.

Keywords- *spoofing, IADLS, pseudo identity, range-free localization, SeRLoc, chaos, RFCA, PWLCM*

*****

I. INTRODUCTION

Recent technological improvements have made the deployment of small, inexpensive, low-power, distributed devices, which are capable of local processing and wireless communication, in a reality. Such nodes are called as sensor nodes. A Wireless Sensor Network is a self-configuring network consists of small sensor nodes communicating among themselves using radio signals, and deployed in quantity to sense, monitor and understand the physical world. Unlike traditional networks, sensor networks depend on dense deployment and co-ordination to carry out their tasks.

Wireless Sensor Networks (WSNs) are used for various applications such as habitat monitoring, automation, agriculture, and security [9]. Since numerous sensors are usually deployed on remote and inaccessible places, the deployment and maintenance should be easy and scalable. Wireless sensor network consists of large number of small nodes. The nodes then sense environmental changes and report them to other nodes over flexible network architecture. Sensor nodes are great for deployment in hostile environments or over large geographical areas.

Due to the openness of wireless and sensor networks, they are especially vulnerable to spoofing attacks where an attacker forges its identity to masquerade as another device, or even creates multiple illegitimate identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin access point attacks. It is thus desirable to detect the presence of spoofing and eliminate them from the network.

In this paper, we address the problem of enabling nodes of Wireless Sensor Networks to determine their location in an un-trusted environment, known as the secure localization problem. We have used a novel range-independent localization algorithm called SeRLoc that is well suited to a resource constrained environment such as a WSN. SeRLoc is a distributed algorithm based on a two-tier network architecture that allows sensors to passively determine their location without interacting with other sensors. We show that SeRLoc is robust against known attacks on WSNs such as the wormhole attack, the Sybil attack, and compromise of network entities and analytically compute the probability of success for each attack. We also compare the performance of SeRLoc with state-of-the-art range-independent localization schemes and show that SeRLoc has better performance. But along with these great features SeRLoc has a drawback that some of the sensor nodes in the network are ignored. To increase the coverage of the sensor nodes we have proposed the new scheme called SeRLoc with Anchors. With the use of this new scheme SeRLoc localization gives the better accuracy position information. For secure and energy efficient communication we used chaos based cryptography in sensor nodes.

II. RELATED WORK

Recently sensor networks are getting more attention because they are low cost and used in intensive applications [2]. Not only in military applications, sensor networks are used in home applications, health applications etc. Sensor networks are dense wireless networks of small, low-cost sensors which collect and dissipate environmental data. Wireless sensor

network facilitates monitoring and controlling of physical environments from remote locations with better accuracy. The environmental conditions may be temperature, sound, pressure. A wireless sensor network is a collection of nodes organized into a cooperative network and to cooperatively pass their data through the network to a main location called base station [3]. The cluster architecture of sensor network sends information from sensor nodes to base station or vice versa [2]. Wireless sensor networks (WSN) are currently receiving significant attention on their limited power and security constraints [4]. Because these wireless networks are limited processing capability due to batteries used in the sensor nodes. And these networks are more vulnerable to attacks due to openness [5].

Hash-based Message Authentication Code (HMAC) [6] is a mechanism for message authentication using cryptographic hash functions. It can be used with any iterative cryptographic hash function such as SHA-1 and MD5, in a combination of a secret shared key. As one kind of Message Authentication Code (MAC), it provides a way for checking the integrity of information transmitted over or stored in an unreliable medium based on a secret key. The use of elliptic curves in cryptography was suggested independently by Koblitz and Miller in 1985. In public key cryptography each user has a pair of keys: a public key and a private key. Only the user knows the private key where as the public key is distributed to all other users. Unlike other popular algorithms such as RSA, ECC is based on discrete logarithms, which consumes more power to provide confidentiality [7]. The AES is a symmetric-key encryption standard [9] provides security that is unbreakable. For ZigBee network, the AES-CTR is very secure, but it is complex and heavy (computational and memory requirements) [10].

Since 1990s, many researchers have noticed that there exists an interesting relationship between chaos and cryptography: many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems [11]. Chaotic functions were first studied in the 1960s and have shown several remarkable properties [20]. Sequences produced by these functions [13] are very random and complex. Poincare was the first to give a clear definition to the term chaos using the example of the spheres. The linear feedback shift register (LFSR) based perturbation technique was proposed [12], [14] to enhance the properties of the digital PWLCM. One common feature shared by all of these sensor networks is the vitality of sensor location. The core function of a wireless sensor network is to detect and report events which can meaningfully assimilated and responded to only if the accurate location of the event is known. So we need a localization algorithm. Localization schemes are classified into two types, direct and indirect approaches [15]. The GPS based localization, in which each sensor is equipped with a GPS receiver. This method adapts well for wireless sensor networks with node mobility. But it is not economically feasible to equip each sensor with a GPS receiver, since wireless sensor networks are deployed with hundreds of thousands of sensors [16]. The indirect approaches of localization were introduced to overcome some of the limitations of GPS based on the nodes position themselves relative to other nodes in their vicinity. Indirect approaches are again classified into range-based [17] and range-independent algorithms [18]. SeRLoc is a range free algorithm that provides secure and energy efficient localization and is most suitable for the MANETS [19].

III. EXISTING SYSTEM

In the existing paper, an Attack Detection and Localization Scheme **(ADLS)** that can detect and localize the multiple identity-based attacks like spoofing and prevent any occurrences of false positives or negatives using Hash keys assigned to different nodes and generated by **EHT** algorithm. It has implemented this scheme for a real time scenario, i.e., 802.15.4 (Zigbee) based Home Security System and evaluated the performance of this experimentation.

In this scheme ADLS uses the combination of MD5 Hash algorithm and HMAC for the detection of attackers. MD5 hash algorithm creates a 128 bit Hash (fingerprint) value, with input as a string of any arbitrary length. The hash represents a kind of signature for the data. Localization is the process of finding the location of the sensor nodes. We use multilateration for localization of sensor nodes. Multilateration can be defined as the process of localization that uses the Time Difference of Arrival, for solving the mathematical intersection of multiple hyperbolas. Here we use a combination of both mean based and median based localization algorithm to find the position estimates of the nodes. In the mean based technique, the coordinates (X, Y) are based upon the positions of beacon nodes (Boi). Let the distance be Doi and the known position is (Xi, Yi). The position (Xo, Yo) of the node can be found out [1]. This may be calculated using the Least Squares Method.

But this ADLS scheme has two shortcomings. First, it uses node identities for attack detection, these node identities can be spoofed easily. Another shortcoming is it uses the GPS system for localization. It becomes a costlier process due to the deployment of GPS receiver at every sensor node.

IV. PROPOSED SYSTEM

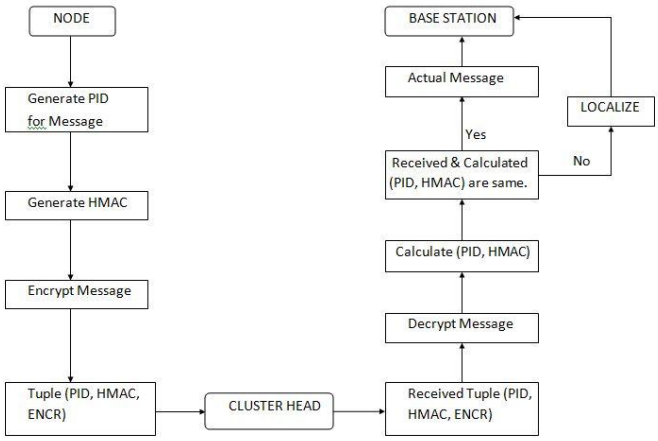
This section consists of our proposed architecture to the improvement of existing method called IADLS(Improved Attack Detection and Localization Scheme), the working mechanism, generalized IADLS algorithm, attack detection, SeRLoc localization, SeRLoc with Anchors and chaos encryption.

 ISSN: 2321-8169
1831 – 1835

A. *Working Mechanism*

This is a different approach to detect identity based attacks like spoofing. In the process of detecting the attack, node generates pseudo identities for individual message. i.e. PID. HMAC is used for authentication. In order to differentiate the attacker node, this scheme uses PID and HMAC of the message. Node also calculates the encrypted message by using chaos encryption with the shared secret key. Now X= {PID, HMAC, ENCR} sent to the base station through the cluster head. Now, the base station decrypts the message by using shared secret key, now, it calculates the HMAC value for the decrypted message and also calculates PID for that message. And now compares them with the received HMAC and PID respectively. If any one of them is not match with respective pair, the base station assumes that the node has been attacked and it invokes the localization scheme. If any node has been attacked, the location of the attacked node is received by the base station, if not actual message is sent to the base station.

Below diagram shows the actual flow of the proposed scheme.



FLOW DIAGRAM FOR IADLS

B. *Generalized Algorithm for IADLS*

Step 1: Generate unique IDs for all nodes in the network.
Step 2:

a) When a node wants to send a message, generate pseudo identity for the message as its unique ID.

b) Generate HMAC code for the message using SHA-1 hash function.

c) Encrypt the message by using the RFCA(Robust and Fast Chaotic Algorithm).

Step 3: Define the cluster, the nodes in cluster and cluster head.
Step 4: Let clusters in network be 'c_n'
Step 5: for (i=0; i<=c_n)

```
{
 AttackerNode=0;
```

I. Decrypt the message

II. Perform spoofing attack detection by checking the message PID, HMAC values.

// calculated and received PID, HMAC values are different, is identified as attack detection.

```
If (Attack Detected)
        {
         If (MESSAGE IS FROM UNCHECKED
                NODE)
           A++;
        }
}
```

Step 6: Perform the detection in every cluster.
Step 7: Identified number of attackers A.
Step 8: Localize the attacker by using SeRLoc with Anchors Algorithm.

C. *Attack Detection using Pseudo Idenities*

1. When a node enters into a network Base Station BS, assigns NID to that node.

2. Now, BS generates two shared secret keys t_i and m_i. it then computes ID of node$_i$ that is verification public key VKP_i = t_i XOR RID. This VKP_i, will passed to the CH to enable it, to verify signatures from N_i even if N_i uses pseudo identity of the message.

3. The BS stores (NID,t_1,mi) tuple and forwards the (VPKi, mi) pair to the cluster head CH. The CH stores the (VPK_i, m_i) pair into its verification table for later usage. It then forwards Ni.

This basically completes the initial handshaking phase. When node Ni leaves the range of a CH and enters the range of another, it includes a simpler authentication process with the BS. BS then generates a new shared secret with Ni and passes necessary information to the new CH for verifying Ni's signature. For details, please refer to [9]. If Ni wants to send and sign a message m_i to a CH Nearby, the following verification procedures will be carried out:

1. Ni first generates a pseudo identity. Different pseudo identities are used for different messages to avoid being traced. To generate a pseudo identity, Ni first generates a random nonce r, then its pseudo identity becomes: PIDi = ($PIDi_1$, PIDi2) = (r × Ppub, VPKi XOR H(miPIDi$_1$)).
2. Ni sends (PIDi, ENCmi (Mi), HMACmi (Mi)) to the CH nearby.
3. Upon receiving the message, the CH finds out Vi's verification public key VPKi and shared secret mi by checking which of stored tuples (VPKi,mi) satisfies the expression PIDi2 = VPKi _ H(miPIDi1).
4. The CH then decrypts ENCmi (Mi) and verifies HMACmi (Mi) using mi. If they are valid, the verification is considered to be successful.

However in our scheme only HMAC checking is involved, and the previous asymmetric encryption of message is simplified to symmetric encryption in our scheme.

D. *HMAC Algorithm*

The second algorithm is for HMAC. HMAC is used by the transmitter to produce the MAC value by combining the single random key 'K' and the message of length' L' [9]. HMAC-MD5 hash algorithm is created from SHA-1 hash function and used as a Hash-based Message Authentication Code (HMAC).The secret key is mixed with the message and the result is hashed with hash function. Again the secret key is mixed with hash value and hash function applied for the second time to get the output of 128 bits in length. The HMAC function may be given as:-

HMACk (y) = f (K' _ opad||f (K' _ ipad||y)) T (1)

To compute the MAC value for the text 'y', the HMAC algorithm is explained as under.

Input: Data String, Secret Key K, Block size S, Inner Pad ipad, Outer pad opad

Output: HMAC function for MAC generation, 128 bit Hash value

STEPS:

Step1: if K=S, set K'=K and go to step 4

Step2: if K>S, apply the Hash function to K and append 0's to get K': K'=H (K) || 00 00…00, then go to step 4

Step3: if K<S, append 0's to end of K to create an S-byte string

Step4: XOR K' with ipad to create an S-byte string: *K' _* ipad

Step5: Append the stream of data 'y' to the string *K' _ ipad* as: *K' _ ipad||y*

Step6: Apply hash function f to the data generated in step 5: *f (K' _ ipad||y))*

Step7: XOR K' with opad: *K' _ opad*

Step8: Append the results of step6 and step7

(K' _ opad||f (K' _ ipad||y))

Step9: Apply hash function f to step8 given as:

f (K' _ opad||f (K' _ ipad||y)) T

Step10: Select the leftmost bytes 'T' of the result generated in step 9 as MAC

E. *SeRLoc Localization*

SeRLoc is a SEcure Range-independent LOCalization scheme. Range-independent localization never tries to estimate the absolute point-to-point distance based on received signal strength or other features of the received communication signal like time, angle, etc. This greatly simplifies the design of hardware, making range-free methods very appealing and a cost-effective alternative for localization in WSNs. Thus, SeRLoc gives a solution to the existing system. In this localization scheme, there are two types of nodes. One is normal nodes and the other one is locators or anchors. Anchors nodes are equipped with directional antennas, and know their location. Normal nodes do not know their location and are equipped with Omni-directional antennas. And each sensor node estimates its location, based on the information transmitted by the anchors. The main idea is the node N_k, within radio range to locators L1, L2, L3 and L4. The working procedure of SeRLoc is as follows.

1. A locator transmits directed beacons within a sector. Each beacon contains the locator's positions and the angles of sector boundary lines. A normal node collects the beacons from all locators it hears.
2. It determines an approximate search area based on the coordinates of the locators heard.
3. It computes the overlapping sector region using majority vote scheme.
4. Finally, SeRLoc determines a node location as the center of gravity of the overlapping region.

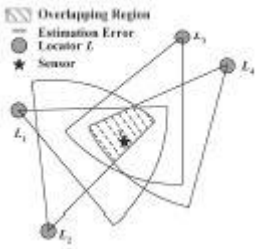


Figure 1. Overlapping region

F. *SeRLoc with Anchors*

SeRLoc is efficient in terms security and power constraints. But it fails in accurate location estimation. The reason is it does not cover all the sensor nodes with in network. The sensor nodes that are not related to any search area, are to be ignored. This causes wrong calculation of exact position. So we need a mechanism that provides accurate position estimation with all the features of SeRLoc. So we proposed a new mechanism that is SeRLoc with Anchors. In this, the whole sensor network is divided into number of regions. And each region should be equipped with at least one anchor. So that, any sensor node within the network must be related with any one of the anchors. Then there is no chance of missing a sensor node. In this way SeRLoc with Anchors provides accurate position estimation.

G. *Chaos Encryption*

The following represents the scheme of the proposed RFCA. The results of the two perturbed PWLCMi, *i* = 1 or 2 (R1 and R2) are combined with a XOR operation to produce a new chaotic stream R with higher randomicity. R is then combined with the plaintext M using a XOR operation. So, the

encrypted data will be given by $C = M$ XOR R. Sharing the initial conditions (the keys), the receiver can generate the same random sequences R1 and R2, compute R and decrypt the received data since XOR is a symmetric operation, by computing: M=C XOR R = (M XOR R) XOR R.

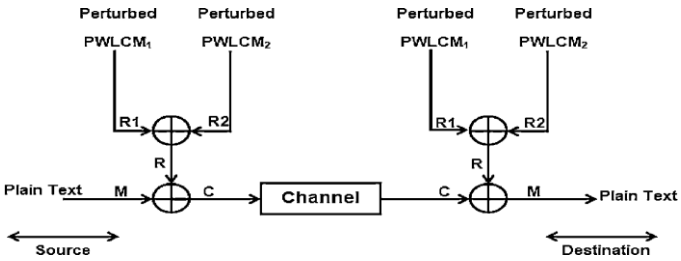


Figure 2. RFCA scheme

V. CONCLUSION

Because the openness of wireless medium and the limited resources, wireless sensor networks are more susceptible to vulnerability of security threats. This paper addresses the identity-based attacks by generating Pseudo IDs to individual messages instead of using node identities. For generating PID this system utilizes the HMAC algorithm. Due to power constraints of sensor nodes this scheme uses chaos based encryption that can be evaluated with fewer computations. SeRLoc with Anchors provides accurate and secure location information. So this paper solely gives the solution to spoofing attacks as well as it is a collaboration of authentication, secure and energy efficient secure communication in wireless sensor networks.

REFERENCES

[1] Ulya Sabeel, Nidhi Chandra, Shivaraj Dagadi "A Novel Scheme for Multiple Spoof Attack Detection and Localization on WSN-based Home Security System" IEEE 5th international conference on Computational Intelligence and Communication Networks,2013.

[2] Archana Bharathidasan, Vijay Anand Sai Ponduru, "Sensor Networks: An Overview" Department of Computer Science, University of California.

[3] H. Karl and A. Willing, "Protocols and Architectures for Wireless Sensor Networks", John Wiely and Sons Ltd, the Atrium, Southern Gate, Chichester, West Sussex, England, 2005.

[4] P.D.M. Bahadurgah, HIT Asodha and U.I.E.T.Rohtak, "Security Threats in Wireless Sensor Networks" IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011.

[5] Ulya Sabeel, Saima Maqbool, Nidhi Chandra, "Categorized Security Threats in the Wireless Sensor Networks: Countermeasures and Security Management Schemes", International Journal of Computer Applications (0975-8887), Volume 64- No.16, February 2013.

[6] C. Zhang, X. Lin, R. Lu, P.H. Ho, "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks", in Proceedings of the IEEE ICC'08, May 2008, pp. 1451–1457.

[7] S. Jarecki, N. Saxena, J.H. Yi,"An attack on the proactive RSA signature scheme in the URSA ad hoc network access control protocol", in: Proceedings of the SASN'04, 2004, pp.1–9.

[8] W. Puech, J. M. Rodrigues, and J. E. Develay-Morice, "Safe transfer of medical images by conjoined coding: Selective encryption by AES using the stream cipher mode OFB and JPEG compression," Ph.D. dissertation, Centre Hospitalier.Changhui Hu, Tat Wing Chim, S.M.Yiu, Lucas C.K. Hui, Victor O.K.Li "Efficient HMAC-based secure communications for VANETs" Journal of computer networks, Elsevier, 2012.

[9] Th. Arampatzis, J. Lygeros, *Senior Member, IEEE*, and S. Manesis, *Member, IEEE* "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks" Proceedings of the 13th Mediterranean Conference on Control and Automation Limassol, Cyprus, June 27-29, 2005.

[10] Gonzalo Alvarez1 and Shujun Li2 "Some Basic Cryptographic Requirements for Chaos-BasedCryptosystems" International Journal of Bifurcation and Chaos, vol. 16, no. 8, pp. 2129-2151,2006.

[11] S. Tao, W. Ruli, and Y. Yixun, "Perturbance based algorithm to expand cycle length of chaotic key stream," *IEEE Electron. Lett.*, vol. 34, no.9, pp. 873–874, Apr. 1998.

[12] S. Li., "Analyses and new designs of digital chaotic ciphers," Ph.D. dissertation, School Electron. Inform. Eng., Xi'an Jiaotong Univ., Xi'an, China, 2003.

[13] G. Chen, X. Mou, and S. Li, "On the dynamical degradation of digital piecewise linear chaotic maps," *Int. J. Bifurcation Chaos August*, vol. 15,no.10,pp.3119–315 1, 2005.

[14] Guoqiang Mao, Barı¸s Fidan, and Brian D. O. Anderson. "Wireless sensornetwork localization techniques". *Comput. Netw.*, 51(10):2529–25532007.

[15] Bo Cheng, Rong Du, Bo Yang, Wenbin Yu, Cailian Chen, and Xinping Guan." An accurate gps-based localization in wireless sensor networks:A gm-wls method". In *Parallel Processing Workshops (ICPPW), 2011 40th International Conference on*, pages 33 –41, sept. 2011.

[16] Wang Jian-guo, Wang Zhong-sheng, Zhang Ling, and Shi Fei. "An improved range-based localization algorithm in wireless sensor network". In Biomedical Engineering and Informatics (BMEI), 2011 4th International *Conference on*, volume 4, pages 2157 –2161, oct. 2011.

[17] Ashok Kumar, Vinay Kumar, and Vinod Kapoor. "Range free localization schemes for wireless sensor networks" In *Proceedings of the 10th* WSEAS international conference on Software engineering, parallel and *distributed systems*, pages 101–106, 2011.

[18] Loukas Lazos and Radha Poovendran. "Serloc: Robust localization for wireless sensor networks" *ACM Trans. Sen. Netw.*, 1(1):73–100, 2005.

[19] A.Awad, S.El Assad, Q.Wang, C.Valdeanu, B.Bakhache, " Comparative study of 1-D chaotic generators for digital data encryption" Int. J. Comput. Sci., vol. 35, no. 4, pp 483-488,2008.