Dos Attack Avoidance Technique For Symmetric Key Algorithm In Wireless Sensor Networks

U. Mekala[1], K. Muthuramalingam[2]
[1, 2] Dept of Computer Science
[1, 2] Bharathidasan University Trichy-23, Tamilnadu, India

Abstract- *Wireless Sensor Networks (WSN) has extensive applications in data gather and data announcement via wireless networks. Due to the weaknesses in the WSN, the sensor nodes are susceptible to most of the security intimidation. Denial-of-Service (DoS) attack is nearly everyone is admired attack on these sensor nodes. Some attack obstacle techniques must be used in opposition to DoS attacks. There are dissimilar techniques to avoid DoS attack in wireless sensor network .In this paper, proposed system for an efficient key establishment scheme to stumble upon several attacks such as denial of service, impersonation attacks which are requisite for the secure interactions in wireless sensor networks. The proposed scheme consists of three stages, namely key-sharing, key-recognition and route-establishment. In the disseminated IoT architecture, sensor nodes and end-users should obtain the capability of securely access a node in a Wireless Sensor Networks.*

Keywords- wireless sensor networks, Key Establishment scheme, denial of service, Attribute based Encryption

I. INTRODUCTION

wireless Sensor Networks (WSNs) have distorted most attractive research part, since it is a useful inbuilt attribute such as small capacity, scalability of nodes, and easy to use. Extensive of WSNs is envisioned to be widely useful in various submissions such as creature path, position checking and data gathering in the neighborhood of future. The WSN is self-infatuated of a huge number of sensor nodes; all sensor nodes are a miniature low-cost wireless mechanism with limited battery-make active power, memory storage and data allowance capacity and short radio announcement range.

Even though description of 'Things' have a changed as knowledge evolved, in that making to computer sense in that sequenced without the aid of human interference remainder the equal. The evolution of the recent Internet into a Network of consistent substance that not only harvest in sequence from the environment (sensing) and interact substantial world (actuation/ authority/control), in that uses existing Internet values to provide services for information transport analytics, applications, and transportation. The devices enabled in wireless technology such as Bluetooth, radio occurrence recognition, the static Internet into a fully integrated for Future Internet [6].

In that assumption ended via these random key pre allocation schemes is that no consumption knowledge is obtainable. The certain deployment knowledge may be accessible a priori, we propose a random key pre-allocation scheme so as to exploits consumption acquaintance and avoids redundant key assignments. The performance of sensor networks can be considerably improved with the use of our proposed scheme [9].

The most destructive and severe attack is Denial of Service (DoS) attack instigate via malicious users on a fatality, a host, a router, or an entire network. It is also achievable that the unauthorized party be forced out of service for some time; the major concern to secure the network is to grip the Denial of Service (DoS) attacks. But there techniques mostly focal point detection to recovery of the system. Improvement of the system is complete after the system is injured. Although the attack is detected system is not much benefit for the absolute state is improvement not guaranteed; Internet of Things (IoT) is a progressively more accepted concept then widely adopted in a wide range of applications, due to the decreasing costs of digital devices and Internet services [10].

Commonly security protocols would provide the Wireless Sensor Network with three capabilities: encryption, authentication, and key management. The Key association is the process by which cryptographic keys are generate, store, susceptible, transfer loaded, used, and demolish. Therefore key management is a critical part of security in WSN and

The compactly investigate freshly. In that WSN, key management protocols can be classified into four categories: symmetric key protocols unauthorized party protocols, and key pre-allocation convention. Denial of Service attacks in wireless data networks have a probable attempt to render impotent the intrinsic worth that come with wireless networks.

II. RELATED WORK

The key factor one must keep in mind when designing wireless sensor network application is energy efficiency of MAC protocol. The MAC protocol must keep the radio in a low-power sleep mode as much as possible [1]. In Roman et al. have found security attacks in distributed IoT. Network entity identity, authentication, access control, and secure communication channel establishment are important security challenges in distributed IoT. Hubaux et al. [2]

The denial-of-sleep attack is a specific type of denial-of-service (DoS) attack that targets a battery-powered device's power supply resulting in quick exhaust of this constrained resource. It is hard to replace those sensors which fail on account of their battery drainage. It is also difficult to recharge those sensors. Thus to effectively increase life of individual sensor nodes and in turn the whole sensor network the battery charge carried by these nodes must be conserved . If we fail to stop the attack, the network lifetime can be reduced from months or years to days [3]. Sensory data [1] associated to myriad of events and occurrences can be analyses and converted into represent able format. Wireless Sensor Network and its security encounters several drawbacks and challenges and they are not properly examined [4].

In that Pair-wise key pre construct schemes, a closest pair-wise keys pre allocation. Scheme and a position based pair-wise keys scheme by means of Attribute based encryption, as a result of taking benefit of sensors' expected position. The analysis in this paper indicates that these schemes can achieve better performance if such position information is available and that the smaller the deployment error (i.e., the dissimilarity sandwiched between a sensor's actual location and its expected position is the better show they can achieve. [8]

The establishment of link-layer keys between neighboring nodes is a fundamental issue in securing sensor network transportation Most of existing solutions are key pre allocation schemes which rely on sensor nodes to broadcast hundreds of or even thousands of pre-loaded key IDs to find pair-wise keys between adjoining nodes [5]

III. PROPOSED SCHEME

The prevent of denial of service attacks, Key mechanisms include random delay for transmissions and passive variation of altering the route through access control nodes and enhance the standard MAC protocol. The proposed scheme consists of three stages, namely key-sharing, key-detection and route-establishment

A. Key Sharing

In which the Key sharing techniques in primary key is engaged for entity endorsement for IoT enable WSNs. In the scattered IoT architecture, sensor nodes and end-users should acquire the capability of securely accessing a node in a Wireless Sensor Networks.

Fresh randomness used for each key generated:

Example:

Public Parameters: $g^{t1}, g^{t2}, \ldots g^{tn}, e(g,g)^{y}$

Ciphertext: $g^{st2}, g^{st3}, g^{stn}, e(g,g)^{sy}$ M

Private key: gy1/t1 , gy3/t3 , gyn/tn

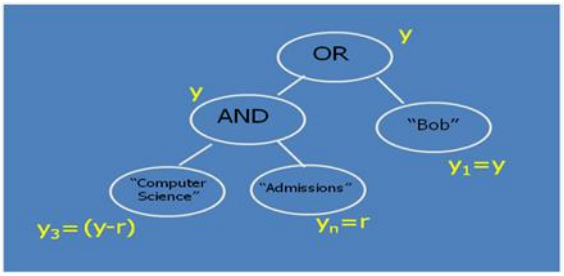

Figure1: key Generation

B. Key detection and Route establishment

The key detection arises for the duration of operational environment in wireless sensor networks. Where all nodes determine its adjacent node in wireless communication through which it detects keys. The efficient method for some two nodes to detect if they share a key is that each node transmission. In this stage, each two of a kind in adjacent nodes to tries locate a shared key that they show. Which key occurs, the key is engaged to secure the announcement link between these two nodes. In which subsequent to key-setup is ended, a linked graph of secure links is created. The key establishment phase of Attribute based Encryption technique allocated with a specific identity for the server.

A separation of such polynomials are then chosen by the server and kept in each of the network nodes. In which the key establishment scheme for period in each sensor node explorers another node with in distribute the identical Attribute based Encryption then both the nodes creates a common key. The main challenge is to establish whether two nodes allocate identical ABE or not.

The real-time discovery nodes can be employed and then ascertain a route with their nearest nodes. If the graph is connected, a route is established from the sender node to its destination nodes or to its adjacent nodes. The sender node can produce route key and send it securely through the pathway to the target node.

Proposed Scheme:

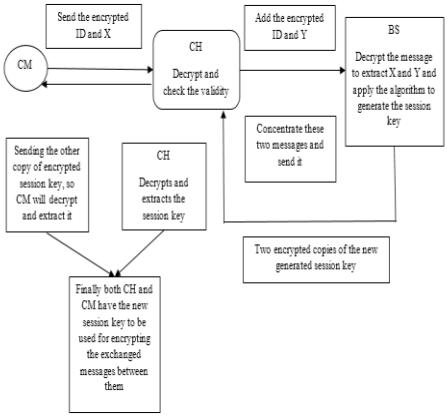

Figure1 Key Generation Process

IV. ATTRIBUTE BASED ENCRYPTION

Attribute-based encryption (ABE) is a moderately recent approach that reassesses the model of public key cryptography. In main features of the complex access control policies can be addressed and the exact list of users need not be known appropriately. Knowledge of the access policy is sufficient. ABE spirit one step further and defines the characteristics not atomic but as a set of attributes e.g., roles and communications can be encrypted with respect to subsets of characteristics (key-policy ABE - KP- ABE) or policies defined over a set of attributes (cipher text-policy ABE - CP-ABE). The key issue is that someone should only be able to decrypt a cipher text if the individual holds.

1) Setup (κ, U)

The input restrictions of this algorithm are the security constraint κ and the space of attribute U. The primitive create a master key MK all along by means of the domain parameters PK.

2) Encryption (PK, M, A)

The set of domain parameters PK, the message M and the access policy a specified as a Boolean formula whose operands are a subset of the universe of attributes are taken as the input for this algorithm. Then, this algorithm encrypts M as the cipher text CT in such a way that only those user who has the set of attributes required to satisfy the access policy A, will be able to decrypt it.

It is assumed that the cipher text and the access policy A must be transmitted together as a pair. (EX) Encodes message M ∈ G1 with a set of characteristics A. Choose a random number s ∈ Zq, and the translated data is available as CT = (A, E = MY s = e (g, g) ys, {Ei = g tis} ∀i∈AU).

3) Key generation (MK, S)

The master key MK along with a set of attributes S is taken as the input in this algorithm. Then, the private key SK is generated with the prescribed set o attributes. Usually, this primitive is executed by a "trusted third party" that has the vital role of generating private key for each one of the participants with a specific access privileges.

4) Decryption (PK, CT, SK)

This prehistoric takes because input the province parameters PK the length of with the cipher text CT and its analogous admittance policy A, and the private key SK, which contains the set of characteristics S. Only in the container that the set of attributes S satisfies the policy A, this primitive will be able to recover the message M from the cipher text CT.

V. RESULT AND ANALYSIS

The result analysis we have created three graphs. In the graphs shown in Figure 2, Figure 3,Figure 4 and Figure 5 in these graphs the x-axis shows the simulation time the y-axis shows the Transmission Analysis, Security Analysis, throughput Analysis and Key Establishment respectively.

The graph in Figure 2 shows the usage of Transmission Analysis during simulation. When the attack takes place the red line shows that the Transmission of Packet the node attacked quickly goes down as the message overhead. Whenever the attack is prevented by carrying out of the Attribute based Encryption algorithm knowledge authentication for nodes sending synchronization messages

Transmission Analysis:

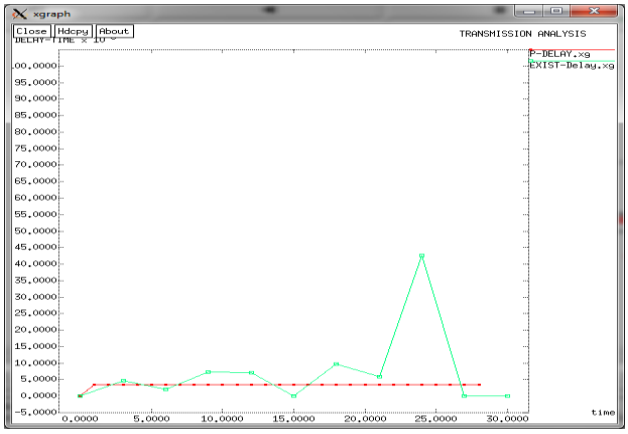

Figure 2: Transmission Analysis with and without attack

Security Analysis:

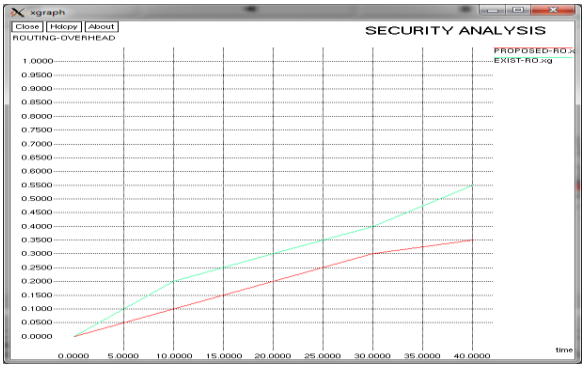

Figure3: Security Analysis With and without Attack

The security analysis between existing and proposed system against DoS attack is analyzed and it is represented in graphical format.

Throughput Analysis:

The throughput value between existing and proposed system is calculated and it is represented in graphical format(X-Graph

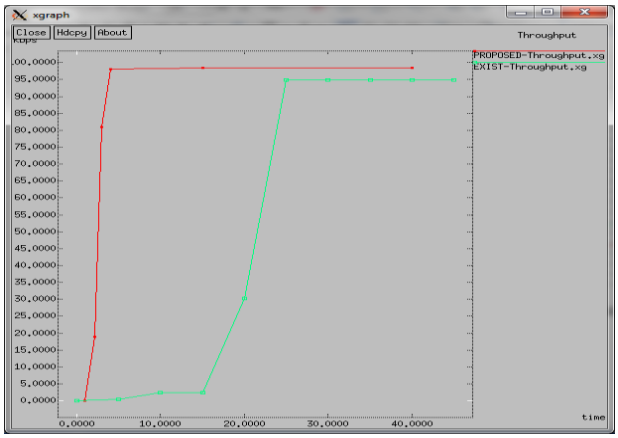

Figure4: Throughput With and without Attack

Key Establishment:

Key Establishment technique is compared between existing and proposed system represented in X-Graph.

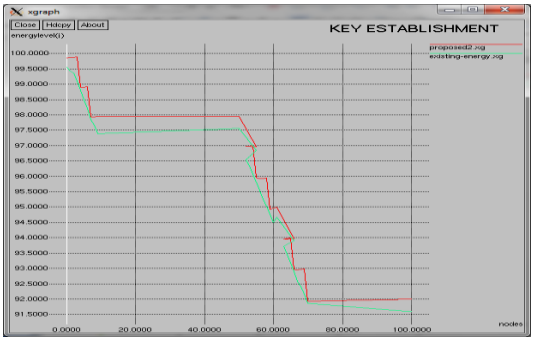

Figure 5: Key Establishment with and without attack

VI. CONCLUSION

In this paper, Dos attack reduces the concert of the system. There are several approaches and technique to prevent DoS attacks on the proposed system for efficient key establishment scheme to stumble upon several attacks such as denial of service, imposture attacks which are necessary for the secure communications in wireless sensor networks. The proposed scheme consists of three stages, namely key-sharing, key-detection and route-establishment in symmetric key encryption. In many conventional networks, a secure key establishment scheme is obviously important to ensure message availability and thereby our scheme guarantees flexibility and less memory cost. Since that future research in plan to further observe on enhancing the network resilience.

REFERENCES

[1] Manju.V.C , Senthil Lekha.S. L. , Dr.Sasi Kumar M. “Mechanisms for Detecting and Preventing Denial of Sleep Attacks on Wireless Sensor Networks”, Proceedings of2013 IEEE Conference on Information and Communication Technologies (ICT2013)

[2] R. Roman, J. Zhou, and J. Lopez, “On the Features and Challengesof Security and Privacy in Distributed Internet of Things,” ComputerNetworks, vol. 57, no. 10, pp. 2266 – 2279, 2013.

[3] David R. Raymond, C. Marchany, Michael I. Brownfield and Scott F. Midkiff, “Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols”,IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 1, JANUARY 2009 367

[4] J. P.Walters, Z. Liang,W. Shi, and V. Chaudhary, “Wireless sensornetwork security: a survey,” in

Distributed, Grid, and Pervasive Computing, X. Yang, Ed., p. 849, CRC Press, 2007.

[5] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M.Yung," Perfectly-secure key distribution for dynamic conferences," In Advances in Cryptology C CRYPTO 92, LNCS 740, pages 471C486,1993.

[6] J. Gubbi, R. Buyya, S.Marusic, andM.Palaniswami, "Internet of Things (IoT): a vision, architectural elements, and future directions,"*Future Generation Computer Systems*, vol. 29, no. 7, pp.1645–1660, 2013.

[7] T. Kothmayr, C. Schmitt, W. Hu, M. Brnig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Networks, ELSEVIER, 2013.

[8] D. Liu and P. Ning, "Location-based pairwise key establishments for relatively static sensor networks," In ACM Workshop on Security of AdHoc and Sensor Networks (SASN'03), October 2003.

[9] W. Du, J. Deng, Y. S. Han, S. Chen and P. K.Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in the IEEE INFOCOM 2004, Hong Kong, March 2004

[10] Fan Wua, Lili Xub, Saru Kumaric An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment," elsevier 2014"