ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

A Secure Trilateration Technique for Cluster Head Localization against Power Exhausting Attacks in WSNs

Vanitha H N[1], B KDeshpande[2], Dr. Suresh L[3]

CSE 4th semester, Dept. of CSE, Cambridge Institute of Technology, Bangalore, India[1]

Asst. Professor, Dept. of ISE, Cambridge Institute of Technology, Bangalore, India[2]

Principal and Professor, Cambridge Institute of Technology, Bangalore, India[3]

ABSTRACT: Wireless Sensor Networks (WSNs) have attracted lots of interests in research and industrial communities. In today's world, a current trend running in industry is the development of WANs. However, effectiveness in transmitting and receiving data the development of sensor techniques makes WSNs a plausible platform of communications that is cheap and easy to deploy. Security and energy efficiency are critical concerns in WSN design. Many media access control (MAC) protocols have been proposed to save the power and extend the lifetime of WSNs; the existing designs of MAC protocol are insufficient to protect the WSNs from denial of- sleep attacks in MAC layer. In order to overcome these types of attacks in this paper we proposed a secure trilateration technique for cluster head localization against power exhausting attacks in WSNs. Method is on the basis of the fact that the known security mechanisms normally awake the sensor nodes before these nodes are allowed to execute the security processes. Therefore, the practical design is to simplify the authenticating process in order to reduce the energy consumption of sensor nodes and enhance the performance of the MAC protocol in countering the power exhausting attacks. This paper proposes a Two-Tier Energy Efficient Secure Scheme integrating the MAC protocol. The outcome describes that in an energy-efficient way the proposed scheme can counter the replay attack and forge attack. The detailed study of energy distribution shows a reasonable decision rule of coordination between energy conservation and security requirements for WSNs.

KEYWORDS: Wireless sensor networks, energy efficiency, denial-of-sleep, power exhausting attacks, Two-Tier Energy Efficient secure scheme.

I. INTRODUCTION

With wide range of potential applications Wireless Sensor Networks (WSNs) are booming technologies now a day. A wireless sensor community is a community of small desktops, sensor nodes those can accumulate knowledge through its sensors, do computations and be in contact wirelessly with different sensor nodes. By and large a wi-fi sensor community is an ad hoc network wherein the nodes arrange themselves without any preexisting infrastructure. Nodes might be deployed randomly, e.g., with the aid of being thrown out from a helicopter over an area that is to be monitored. As soon as within the area, the nodes that survived the deployment system keep up a correspondence with the other nodes that occurred to end up in its neighborhood, and they set up an infrastructure. The performance of WSNs is performed and boosted by optimizing the power consumption. Safety measures and energy efficiency are the most significant concerns in wireless sensor networks (WSNs) design. To accumulate the power and enlarge the lifetime of WSNs, a range of media access control (MAC) protocols are proposed. Most conventional security solutions cannot be functional in the WSNs due to the constraint of power supply. The well-known safety measures mechanisms usually aware the sensor nodes before the sensor nodes can affect the security processes. In recent years, lots of WSN applications have shifted from specific fields to domains related to people's daily lives such as health care, and intelligent home, where a variety of wireless devices coexist.

DOI: 10.15680/IJIRCCE.2016. 0404347

The Denial-of-Sleep is among the energy hard attacks of WSNs. This assault is a distinctive style of Denial-of-provider (DoS) attack, which tries to hold the sensor nodes conscious to eat extra vigour of the restrained vigour deliver. An anti-node can send false data packets to sensor node of unprotected WSNs to initiate unnecessary transmissions again and again. Without protection mechanism, an anti-node can broadcast a fake preamble probably within the sender-initiated schemes. If the receiver can't tell the true preamble and the false one, the receiver will obtain and approach the information from the anti-node. Such attack will preserve the receiver conscious as long as the info transmission sustains, which exhausts the battery of nodes quickly. In addition, an anti-node can replay a false preamble ACK to the sender. Consequently, the sender will begin to ship the info to the anti-node however it will not ever acquire the proper knowledge ACK. In a similar way, the sender may send data many times and exhausts the battery of node quickly. In receiver-initiated schemes, an anti-node can broadcast a “fake beacon” to cheat sender to method and ship the info to the anti-node but it's going to not ever obtain the correct knowledge ACK. An anti-node can replay a “false beacon ACK” to the receiver. As a consequence, the receiver will to receive and approach the information from the anti-node. If the interval of assault packets is shorter than the sleep interval of a WSN, then the verbal exchange between neighboring nodes in a WSN might be interfered by using assault packets.

The RI-MAC protocol is one of the receiver-initiated schemes to cut down the channel occupancy time of a pair of a sender and receiver, which enables the sender to send information to the receiver as soon as it senses the beacon. Nevertheless, present layer-2 protocol designs are inadequate to guard a WSN from Denial-of-Sleep attack. The vigour conservation is one in all the predominant goals of WSN design, whereas the protection scheme constantly consumes more power of system. There is no well selection rule to compromise the requisites between power conservation and protection scheme.

This paper proposes a two-tier energy efficient secure transmission scheme. In order to generate the dynamic session key this scheme uses the hash-chain, which can be utilized for mutual authentication and the symmetric encryption key. The only computations of dynamic session key are the hash services, equivalent to MD5 or SHA-1, that are very simple and speedy. With the aid of integrating with MAC protocol, there is not any extra packet in comparison with the present MAC designs. The 2-tier design can assess and interrupt the assaults at specific investigate facets. The mixture of low complexity protection procedure and a couple of check points design can defense against attacks and send the sensor nodes again to sleep mode as soon as viable. The safety analysis shows that this scheme can counter the replay attack and forge attack, and the vigor evaluation indicates that this scheme is energy efficient as good. The exact vigor distribution of power analysis also indicates a new viable resolution rule to compromise the wishes between vigor conservation and protection scheme.

II. Literature Survey

S.Manikandan et al. [1] has proposed a Energy-Efficient Secure Key Distribution System In Hierarchical Wireless Sensor Networks. In this their main objective is to propose a cross-layer design of secure scheme incorporate the MAC protocol. Assigning trust values to the nodes based on energy level. Interactions between nodes are performed by study of expectation value and multiple hops are selected according to, nodes having better trust value. The study shows that the proposed scheme can argue against the replay attack and forge attack in an energy-efficient way.

Zygmunt J. Haas et al. [2] has developed a Current Challenges and Approaches in Securing Communications for Sensors and Actuators. In this they provide background material on WSN security; in particular, we present the security goals, implementation constraints, potential attacks and defenses, and evaluation benchmarks and they discussed on basic security challenges and approaches, including cryptography schemes, key management schemes, and attack detection and prevention mechanisms and also about secure routing, secure localization, and secure data aggregation, respectively. Finally, they concluded the proposed syatem.

Andreas Larsson et al. [3] have proposed Security and Self-stabilization in Sensor Network Services. In this paper they have provided a common way is to cluster the nodes together into groups which are used by many applications and other fundamental services. They presented a self-stabilizing algorithm for clustering. It uses redundant paths to be resilient against captured nodes in the network. It assumes perfect message transfers and lock step synchronization of the nodes. In addition, we present a clustering algorithm that is a further development of that work that can handle unreliable communication media and unsynchronized nodes assuming a limit on clock rate differences.

DOI: 10.15680/IJIRCCE.2016. 0404347

III. METHODOLOGY

Figure 1 represents the proposed architecture. The architecture first starts working for the left palmprint images and . Fistly will deploy the WSNs where we selecxt the sensor nodes and these sensor nodes are subjected to secure topology formation phase where Once the network deployment is done with selection of sensor nodes will move for anti-node detection using authenticated broadcasting mechanism, as for secured network there should not be any anti-nodes present in the network The good network must be robust so in order to make the network robust against attacks, an authenticated broadcasting mechanism, namely the µTESLA in SPINS may be needed in anti-node detection phase. As soon as we gained a network topology without anti-nodes we have to use adaptive allotted topology control algorithm (ADTCA) scheme, in this scheme there are two important subsections are there, they are cluster head selection and gateway selection, next, two symmetric shared keys, a cluster key and a gateway key, are encrypted by way of the pre-distributed key and are dispensed locally. After the secure topology formation stage, there is a shared secret key between the valid member nodes and cluster head of each cluster. Based on the secure cluster topology, a two-tier security scheme is performed to transmit information securely and quickly. This scheme can assist the nodes in deciding to switch into sleep mode or to keep awake as soon as possible. Thus we achieve the aim of our proposed system.

A. SECURE TOPOLOGY FORMATION STAGE

In this stage, the relaxed secure adaptive topology control algorithm (SATCA) is involved to form the hierarchical topology in four phases; they are anti-node detection, cluster formation, key distribution and key renewal. This preliminary research constructs the clustering topology with a secret key shared with the aid of the cluster head and its cluster participants in a cluster. Observe that a cluster member can handiest be in contact with its neighboring nodes having the same cluster membership, which avoids broadcast-like conversation inside clusters. Once the network deployment is done with selection of sensor nodes will move for anti-node detection using authenticated broadcasting mechanism, as for secured network there should not be any anti-nodes present in the network so after achieving anti-nodes free network topology by using ADTCA scheme will create cluster formation. Next, by using encryption of cluster formatted key and gateway key will do key distribution and by using cluster heads will achieve key renewal. Thus we can form secure topology.

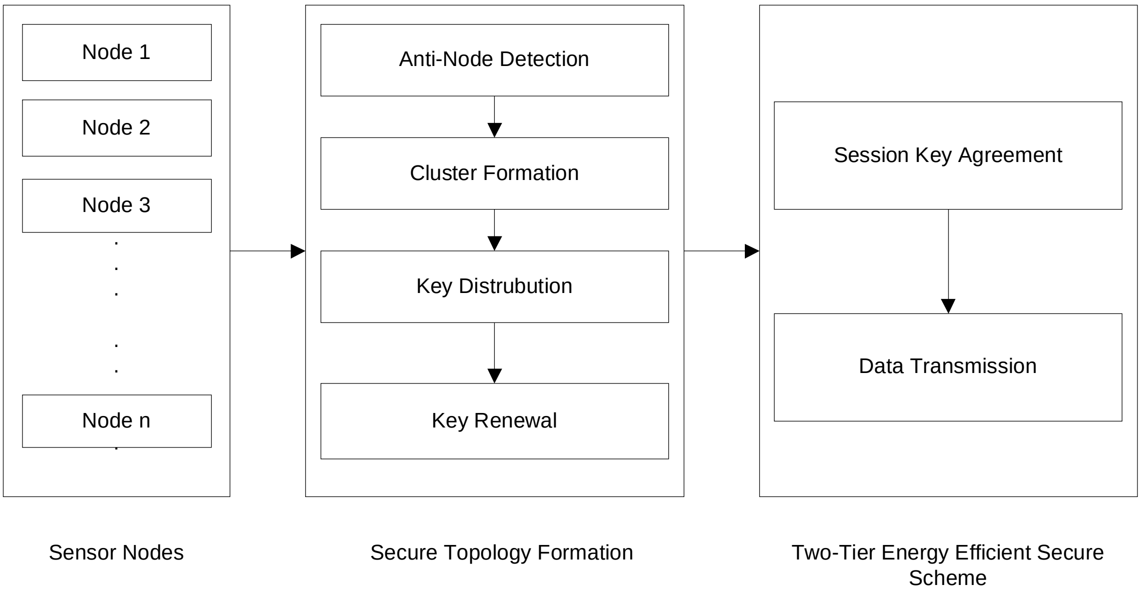


Figure 1: Block Diagram of Proposed System

I. ANTI-NODE DETECTION

Once the network deployment is done with selection of sensor nodes will move for anti-node detection using authenticated broadcasting mechanism, as for secured network there should not be any anti-nodes present in the network The good network must be robust so in order to make the network robust against attacks, an authenticated broadcasting mechanism, namely the µTESLA in SPINS may be needed in anti-node detection phase. In the authenticated broadcasting mechanism, as the broadcasting challenge a normal “Hi” message is encrypted by the pre-distributed key. The sender is said to be an anti-node when sensor cannot decrypt the received message successfully. Thus, the normal nodes and the anti-nodes can be differentiated from one another. As for more security network topology must be free of anti-nodes, therefore, we keep on the network topology without anti-nodes in order to make the network safe. By operating in this phase 1 we can control the external attack. In this work, we do not have a lightweight counter measure to defend against authenticated malicious nodes. If the authenticated node is compromised and performs malicious activities, a mechanism for evicting the compromised nodes is required.

II. CLUSTER FORMATION

As soon as we gained a network topology without anti-nodes we have to use adaptive allotted topology control algorithm (ADTCA) scheme, in this scheme there are two important subsections are there, they are cluster head selection and gateway selection

1. CLUSTER HEAD SELECTION:

Each sensor sets a random waiting timer, proclaims its presence by way of a “hi” sign, and listens for its neighbor’s “hi”. The sensors that hear many neighbors are just right candidates for initiating new clusters; those with few neighbors should select to wait. Sensors update their neighbor understanding and lessen the random ready time centered on each “new” what’s application message acquired. This encourages those sensors with many neighbors to come to be cluster heads. If a neighbor broadcasts itself to be a cluster head, the sensor cancels its possess timer and joins the neighbor’s new cluster. If the timer expires, then the sensor proclaims itself to be a cluster head, a focal point of a new cluster. By means of adjusting randomized ready timers, the sensors can coordinate themselves into shrewd clusters, which will then be used as a basis for additional communication and information processing. After making use of the ADTCA, there are three distinctive sorts of sensors will be formed, firstly the cluster heads, secondly sensors with an assigned cluster identification, finally sensors without an assigned cluster id, so that they can join any local cluster and grow to be 2-hop sensors. The topology of the ad-hoc network is represented with the aid of a hierarchical assortment of clusters.

2. GATEWAY SELECTION

There are many non-overlapping clusters will be present in the network so in order to interconnect two adjacent non-overlapping clusters, one cluster member from each cluster must become a gateway. As in the procedure of cluster formation, sensors can obtain local information and know the number of neighboring sensors in adjacent clusters. Therefore, for gateway selection sensors may initialize their counters in the given local information, Based on the counter, cluster heads broadcast messages to trigger the gateway selection process. After applying the procedure for determining gateways, the gateway nodes broadcast messages to update the connectivity information and activate the linked cluster architecture. The result of the cluster formation processing is that each cluster i assign a single member to communicate with each nearby cluster j.

III. KEY DISTRIBUTION

On this phase, two symmetric shared keys, a cluster key and a gateway key, are encrypted by way of the pre-distributed key and are dispensed locally. A cluster secret's a key shared by means of a cluster head and all its cluster participants, which is most of the time used for securing in the community broadcast messages, routing control expertise, or securing sensor messages. Furthermore, so as to type a comfy verbal exchange channel between the gateways of adjacent clusters, a symmetric shared key is also used to encrypt the sending message. On this phase, a further project encrypted by means of a cluster key or a gateway key could also be made to look after against anti-nodes which have now not been discovered in previous phase. Accordingly, the security of intra-cluster conversation and inter-cluster conversation are based upon a cluster key and a shared gateway key, respectively. Now the function of safety key is surpassed over to cluster key and gateway key. After the cluster key and gateway key are created, the pre-allotted key may also be ignored in case a node is hijacked and the pre-allotted key is compromised.

IV. KEY RENEWAL

To preserve the sensor network and preclude the adversary from getting the keys, key renewing is also fundamental. At the start all cluster heads (CHs) choose an originator to begin the “key renewals”, and then it'll ship the index to all cluster heads within the community. After picking out the originator, it initializes the key renewal procedure and sends the index to its neighboring clusters by gateways. Once we got the Clusters Heads, all cluster heads chosen originators to start key renewal; it will send the index to all cluster heads in the network. The cluster heads refreshes the two keys from the key pool, and distributes the two new keys to their cluster members locally. The operation repeats the way through to all clusters in the network.

B. TWO-TIER ENERGY EFFICIENT SECURE SCHEME

After the secure topology formation stage, there is a shared secret key between the valid member nodes and cluster head of each cluster. A cluster key is a key shared by a cluster head and all its cluster members, which is mainly used for securing local broadcast messages (e.g. routing control information or sensor messages). Based on the secure cluster topology, a two-tier security scheme is performed to transmit information securely and quickly. This scheme can assist the nodes in deciding to switch into sleep mode or to keep awake as soon as possible. The proposed cross-layer design, Two-Tier Energy-Efficient Secure Scheme (TE2S), integrates the MAC protocol and involves coupling two layers without creating new interface for information sharing at runtime, which aims to protect the WSNs from Denial-of-Sleep attack. There are two important subsections in two-tier energy efficient secure system they are session key agreement known as tier 1 and data transmission known as tier two.

1. TIER-1: SESSION KEY AGREEMENT

After the network topology formation stage, there's a shared secret key between the valid member nodes and cluster head of each cluster. A cluster secret is a key shared by way of a cluster head and all its cluster participants, which is generally used for securing regional broadcast messages. Founded on the at ease cluster topology, a two-tier safety scheme is performed to transmit understanding securely and quickly. This scheme can guide the nodes in figuring out to switch into sleep mode or to preserve conscious as quickly as feasible.

The communiqué initiator can be the sender or receiver, which depends upon the design of scheme. We form the participators as originator and replier in one-of-a-kind schemes. To determine the secure token valid, the replier has to execute 1 hash function computing and 1 comparing computing. To verify the replier is valid, the originator computes and compares the got h(h(Ks)). These computations are very easy and speedy. If the comfy token or h(h(Ks)) will not be valid, the information receiver goes back to sleep mode instantly and discards the entire relaxation approaches, also the data sender will no longer send the information. The hash chain h(Ks) and h(h(Ks)) are computed for mutual authentication. As a consequence, the sender and receiver attain a dynamic session key agreement with just one random quantity decision and three hash perform computations, respectively. The dynamic session keys are created in the session key agreement tier at the same time the packet exchanging tactics are performed in every key contract operation. The newly chosen random quantity ensures that no session keys can be reused. Become aware of that this key contract does no longer contain any encryption/decryption. The random number is the perform of timer to make the operation of the random quantity generator easy and speedy.

2. TIER-2: DATA TRANSMISSION

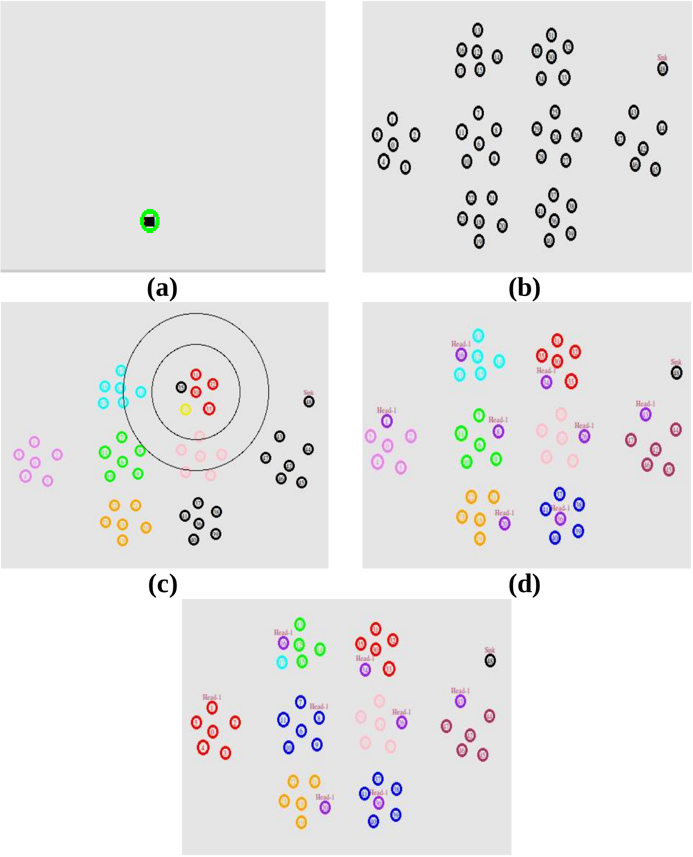
The session key Ks is the new created dynamic key, the sender can encrypt the transmission data via symmetric encryption. Implementation is explained below

The sender sends the h(Ks)and EKs(knowledge MACKs (data) to receiver, theEKs (x) denotes encrypts x by using utilizing symmetric algorithm with key Ks. The MACKs (knowledge) denotes the message authentication function with key Ks, the place knowledge is the input message. The receiver verifies the h(Ks). If the h(Ks) just isn't valid, the receiver goes back to sleep mode instantly. If the h(Ks) is valid, the receiver decrypts the information and assessments the MAC of data.

The receiver sends the info ACK to sender. Hence, the sender computes h(Ks) from recognized Ks or Kc. To determine the got packet valid, the receiver best comparesh(Ks). If the h(Ks) just isn't legitimate, the receiver goes back to sleep mode immediately and discards all of the leisure procedures. It is infeasible to compute the h(Ks) from h(h(Ks)). The sender must compute h(Ks) from recognized Ks or Kc. the hash chains h(Ks) and h(h(Ks) authenticate sender and receiver jointly.

C. EXPERIMENTAL RESULT

Figure 2 represent the overall experimental result of proposed work. As we started with sensor nodes selection which is show in Figure 2(a), next these sensor nodes are subjected to cluster formation as show in the Figure 2(b) during cluster formation there are two stages are there in which selection of cluster heads is one among the two as shown in Figure 2(e) and Figure 2(c) represent that the sensor cluster formatted nodes sending messages to neighbor nodes. After the selection of cluster head selection there we have to select the gateway for the nodes, finally will get performance analysis graph which can give us throughput, energy consumption and pocket sending node as demonstrated in Figure 2(f), 2(g) and 2(h) respectively.



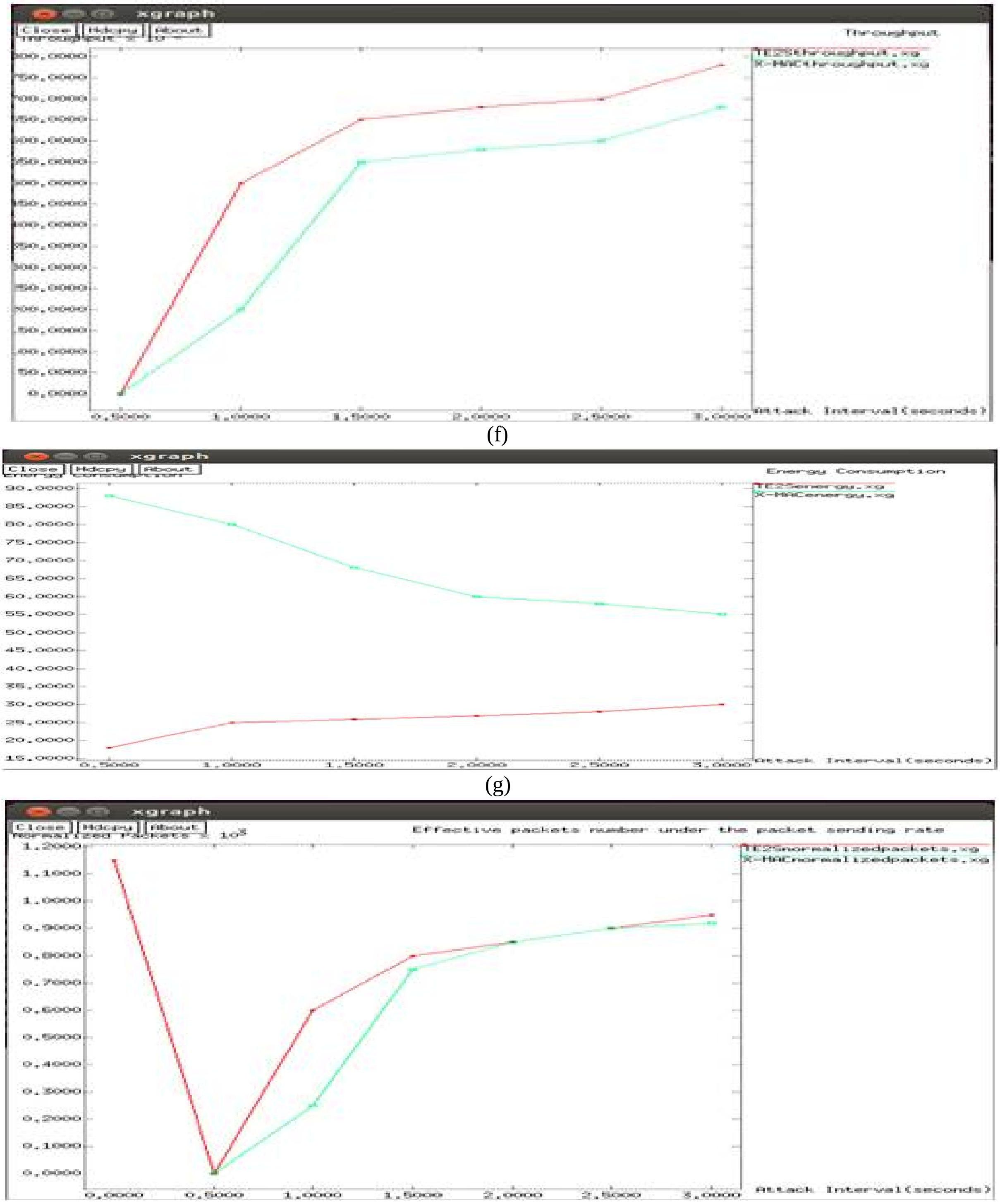
(a)

(b)

(c)

(d)

(e)



(f)

(g)

(h)

Figure 2: (a) Sensor Node; (b) Cluster Formation; (c) Sending MSG to neighbor Node; (d) Sending Node; (e) Cluster Head selection; (f) Throughput Graph; (g) Energy consumption Graph; (h) Packet sending rate.

DOI: 10.15680/IJIRCCE.2016. 0404347

D. CONCLUSION

This paper proposes a cross-layer design of vigour-efficient scheme integrating the MAC protocol. No additional packet is worried within the fashioned MAC protocol design. This scheme can scale back the authenticating method as quick as viable to mitigate the outcomes of the vigor onerous assaults. By way of blend of low complexity security procedure and multiple check elements, the proposed design can safeguard against assaults and ship the sensor nodes back to sleep mode as soon as possible. The security evaluation indicates that this scheme can counter the replay assault and forge assault. The vigour evaluation identifies the running mode exactly, including the MCU and radio modules. The simulation outcome of normalized vigour consumption for common situation, which has no attacks, show that the proposed scheme increases lower than 2.57% in vigour consumption of the X-MAC protocol and no more than three. Sixty three% in energy consumption of the RI-MAC protocol with various packet sending rates. The simulation outcome of normalized energy consumption for attack conditions additionally exhibit that the proposed scheme can store instances of vigor consumptions than X-MAC or RI-MAC does, which may also lengthen the lifetime of WSNs beneath assaults. The power evaluation shows that this scheme is efficient in both sender-initiated scheme and receiver-initiated scheme. The overall results exhibit that the proposed at ease TE2S scheme can achieve the equal throughput performance with much less vigor consumption. Additional energy consumption of the proposed scheme beneath more than a few responsibility cycles may also be investigated to furnish extra huge simulation results to aid the effectively of TE2S scheme one day.

REFERENCES

[1] S.Manikandan, V. Nagaraj, B. Prabakaran, R. Sathiskumar, "Energy-Efficient Secure Key Distribution System In Hierarchical Wireless Sensor Networks", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 12, December 2015.

[2] Zygmunt J. Haas, Lin Yang, Meng-Ling Liu, Qiao Li, and Fangxin Li, "Current Challenges and Approaches in Securing Communications for Sensors and Actuators", Cornell University, Ithaca, 2014.

[3] Andreas Larsson, " Security and Self-stabilization in Sensor Network Services", Division of Networks and Systems, Chalmers University of Technology, Vol. 2, 2015.

[4] Y. Wu and Y. Li, "Construction algorithms for k-connected m-dominating sets in wireless sensor networks," inMobiHoc '08, New York, NY, USA, 2008, pp. 83–90, ACM.

[5] K. Sun, P. Peng, P. Ning, and C. Wang, "Secure distributed cluster formation in wireless sensor networks," in ACSAC '06, Washington, DC, USA, 2006, pp. 131– 140, IEEE Computer Society.

[6] A. Larsson and P. Tsigas, "A self-stabilizing (k,r)-clustering algorithm with multiple paths for wireless ad-hoc networks," in ICDCS 2011, Minneapolis, MN, USA, 2011.

[7] C.-T. Hsueh, Y.-W. Li, C.-Y. Wen, and Y.-C. Ouyang, " Secure adaptive topology control for wireless ad-hoc sensor networks," Sensors, vol. 10, no. 2, pp. 1251–1278, 2010.

[8] M. Li, Z. Li, and A. V. Vasilakos, "A survey on topology control in wireless sensor networks: Taxonomy, comparative study, and open issues," Proc. IEEE, vol. 101, no. 12, pp. 2538–2557, Dec. 2013.

[9] Y. C. Ouyang, C. T. Hsueh, and H. W. Chen, "Secure authentication policy with evidential signature scheme for WLAN," Security and Communication Networks, vol. 2, no. 3, May/June 2009, pp. 259-270.