Certifying Truthfulness using a Light-Weight Security System in Clustered Wireless Sensor Networks

A.B. Ashin Leo[1] B. Anusha[2]

[1,2]P.G. Student

Abstract— Wireless Sensor Networks are deployed in an area where the humans are not able to access, security becomes more important because they are prone to many types of attacks. WSNs are more susceptible to attacks mainly due to the nature of their deployment and the mode of communication. The proposed model is a light weight security scheme capable of maintaining all the security features such as confidentiality, integrity and protection against replay attack. The proposed model aims to prevent replay attack and provides integrity within the network by sending query to every phase of communication. To provide replay attack protection, an extended model known as MSQPS (Modified Secure Query Processing Scheme) is used. In MSQPS, once the network starts to process a query no new node can join the network until the query is processed. MSQPS provides security to the stored data in nodes and the communication among the nodes. The limitation is that the probability of attacking cluster head and the member nodes is higher than attacking the base station. In all communication between the cluster heads and member nodes the key is neither transmitted nor pre-deployed. It protects the replay attack and provides the basic security features such as the confidentiality and integrity. The performance of the scheme is evaluated through data freshness, authentication rate and packet delivery ratio and so it provides better integrity level.

Key words: Wireless Sensor Networks, Authentication, Attacks, Query Processing

I. Introduction

The modern field of Wireless Sensor Networks (WSN) combines sensing, computation and communication into a single small device. The power of wireless sensor networks lies in the capability to deploy large numbers of small nodes that gather and organize themselves. The straight onward application is to monitor remote environments for small frequency data trends. For example, a chemical plant could be easily monitored for leaks by hundreds of sensors will automatically forms a wireless interconnection network and immediately report the detection of any chemical leaks. A WSN consists of tens to thousands of nodes.

The sensor nodes in the network can also be known as motes, these sensor nodes have the capacity to perform some processing, colleting sensor related information's and also performs communication with other connected nodes in the network. In sensor nodes the mote can be a node where the node will not be a mote. Currently, motes are focusing on developing the largest wireless range that is in the range of dozens of Kms, the lesser energy conservation and the easy improvement process for the users.

Some of the components in sensor nodes are microcontrollers, transceiver, external memory, power source and one or more number of sensors.

The sensor networks are mostly used in areas such as military force, health monitoring, control in industries, controlling of homes and so on. In military force the sensor networks are used to monitor the entry of enemy country people attacks and the informations related to the country are being monitored.

Industries makes use of sensor nodes to monitor the industrial informations such as the chemical leackages, power supply etc. controlling of homes are used to find the theif entering the homes the misbehavior of the person using their activities and so on.

WSN is a network of small sensor nodes communicating among themselves using radio signals and also used to sense, monitor and understand the physical world. It acts as a communication link between the real physical and the virtual world. It had a wide range of applications to industry, science, transportation, civil infrastructure and security. The sensors are used to monitor temperature, humidity and light etc.

WSN's are scalable and requires very little power. It is a single purpose design it means that it can serve one specific application. It has the ability to work in environments with harsh conditions. It consists of a base station or a gateway to communicate with a number of sensor nodes through a radio link.

A. *Characteristics of WSN*

1) WSN has the ability to work with node failures it means that if one node gets failed then the remaining nodes will not stop working.
2) Every node is equipped with smart sensors which can communicate with each other without any specified infrastructure

The drawback of sensor network is that they makes use of batteries. Since these nodes are deployed over the large number of areas the batteries will soonly become die. Changing or recharging of sensor batteries are very difficult. WSN's are susceptible to attacks due to the nature of their deployment and mode of communication so that security has become more important. Attacks in WSN is of two types namely active attacks and passive attacks.

In active attacks the adversaries will listen and then modifies the communication that takes place in the network. In passive attacks the attackers only eavesdrop the communication in the network without actively participating in the distributing the communication.

II. Related works

Yafeng Wu, Matthew keally, Gang Zhou, Weizhen Mao – "Traffic Aware Channel Assignment in Wireless Sensor Networks" 2009 focuses on channel assignment problems in sensor networks. The prevailing persistent method for channel assignment are inadequate because they diminish the potential interfering with the assumption that all nodes have the identical amount of energy to convey concurrently and also a section of nodes needs to spread energy at the same rate. Even a specific sensor network is deployed, the traffic volume and pattern vary significantly across the placement area and through time. For the improvement of current channel assignments, the new channel assignment scheme adventures traffic information to minimize interference occurring with real traffic. Traffic-aware can increase the performance of channel assignment. It helps to establish the potential benefits of traffic-aware channel assignment algorithms.

Yi Ouyang, Zhengyi Le, Guanling Chen, James Ford, Fillia makedon – “Entrapping Adversaries for Source Protection in Sensor Networks” 2000 have discussed the problem of protecting source locations in sensor networks. A cyclic entrapment approach is developed to lead the adversaries into traffic loops in a sensor network. The source location will get protected when adding a low cost in terms of message latency and energy usage. The advantage of using cyclic entrapment method is that it protect the source’s location when allowing for an optical routing time for messages from that source.

Vinidha Roc, Dr. Ajay D.Vimalraj, C. Maria Antoine Pushparaj – “Energy Efficient Protocol with Static Clustering (EEPSC) Comparing with Low Energy Adaptive Clustering Hierarchy (LEACH) Protocol” 2013 focuses on describing a novel hierarchical with static clustering routing protocol called Energy Efficient Protocol with Static Clustering that partition the network into static clusters to eliminate the overhead of dynamic clustering. For extending the network lifetime it utilizes the temporary cluster heads to distribute the energy among the high power sensor nodes. Finally EEPSC will have a better network life time and minimum power consumption in terms of LEACH.

Nangai Abinaya S, Sudha R – “A Clustering Mechanism for Energy Efficient Routing Path” 2014 focuses on developing a link-aware clustering mechanism called LCM to determine the energy efficient routing path. It introduces a Predicted Transmission Count (PTX) to construct the cluster structures as a clustering metric to determine the priority for every cluster heads. Based on these derived priorities LCM will select the optimized nodes. Finally LCM will consider the energy usage and link condition values for constructing a routing path that guarantees the report quality and so it achieves a better energy consumption, packet delivery ratio and the throughput.

Nitin Jain, Samir R.Das, Asis Nasipuri – “A Multichannel CSMA MAC Protocol with Receiver-Based Channel Selection for Multihop Wireless networks” focuses on developing a CSMA based MAC (Medium Access Control) protocol for a multi hop wireless sensor networks that makes use of a multiple channel and a dynamic channel selection method. It uses one control channel and N data channels that is it can have independent number of nodes in the network.The selection of channel is based on maximizing the signal to interference and the noise ratio at the receiver so the network will have a lower delay and higher throughput in static grid networks.

G.S.R Emil Selvan, S.Sivagurunathan, P.Subathra, S.Dina Nithya “Mobile Ad hoc Network Security - A Cluster based Approach” 2009 describes a threshold security mechanism with a mobility based D-hop clustering algorithm that measure the variation of distance between nodes over time. The threshold scheme will protect routing information and the data traffic. To ensure the trust in clustered environment, the private key is divided into n number of pieces so that the private key can get easily reconstructed.

Devender Thakur, Amit Nayyer – “Multichannel Communication – A Need for Wireless Sensor Networks” 2014 [7] has developed a multichannel communication. By using multichannel communication, the adjacent nodes in the network can transmit their packets at the same time through different channels so that those channels will not interfere with each other. They not only improve network throughput and capacity but also it reduces the collisions and interference. It provides better choice for WSN MAC protocols and it also supports multimedia data transmission.

Jingbin Zhang, Gang Zhou, Chengdu Huang, Sang H. Son, John A. Stankovic [8] “TMMAC: An Energy Efficient Multi-Channel MAC Protocol for AdHoc Networks” focuses on developing a energy efficient multi-channel MAC protocol using a single half duplex radio transceiver based on TMMAC protocol. It introduces a lightweight explicit time negotiation to achieve a greater power savings by allowing the nodes that are involved in communication. Finally a improved communication overhead and energy savings will be obtained.

Hitesh Matre “A Survey of Key Pre Distribution Scheme for Wireless Networks” [9] 2014 focuses on presenting a pre key distribution in the WSN. The key is pre distributed in three phases namely key distribution, shared key discovery and path key establishment. During these phases, the secret keys will get generated and a secret link is established when two nodes discovers one or more common keys and the communication will also done between these nodes. Since the key is pre distributed the WSN will have higher scalability, good key sharing key probability, and also the storage overhead gets reduced.

Shih I Huang, Shiuhpyng Shieh, J.D.Tygar [10] “Secure Encrypted-data aggregation for Wireless Sensor Networks” 2010 focuses on providing a secure data aggregation scheme for WSN. Without encryption it eliminates redundant sensor readings for the aggregated data and also maintains data secrecy and privacy during transmission. Here the duplicate instances of original readings will be aggregated into a single packet. It is resilient to the known plain text attacks, chosen plain text attacks and man in the middle attacks so that the communication overhead will get reduced.

III. SYSTEM DESIGN

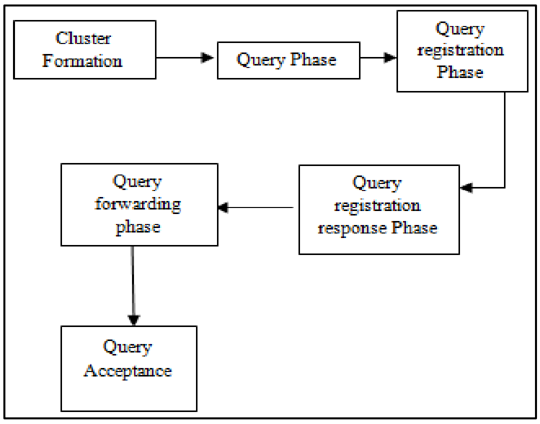


Fig. 1: Architecture of the Proposed Model

Fig 1.1 depicts the architecture model of the proposed system. Here the clusters are initially formed and then it goes to the query phase which includes the phases as query registration phase, query registration response phase, query forwarding phase and finally the query acceptance.

IV. PROPOSED MODEL

In this model the nodes in the network are initially randomly deployed and then the randomly deployed nodes are formed into clusters to lesser the amount of energy used. The clusters are formed using the method as LEACH.[11]. The nodes in the network will form themselves into cluster as one node as the Cluster Head(CH) and the continuing nodes as Cluster Node (CN). Once the Clustered network is made and the nodes are registered then the query phase is established from the Base Station (BS) to CH and then from CH to CN.

A. *Query Phase*

The query phase among BS and CH is used to confirm the query message advertised from BS to CH. BS will transmit a 8-bit query message. This 8-bit query is XORed with $T'_{BS-recent}$ and the result H_E is obtained then the resultant H_E is complented to obtain H'_E. After complement the most significant bits (4 bits) from H is swapped with the smallest weighty bits (4 bits) of H'_E then H and H'_E are concatenated to obtain the encrypted query packet H''_E.

CH will receive H''_E and then performs decryption by swapping, splitting and computing of H and then resultant H'_E is obtained. H'_E is complemented to form H_E. Finally, H_E and the original H are XORed to obtain $T'_{BS-recent}$ if the obtained value equals $T_{BS-recent}$ stored in CH then the message from BS is confirmed.

CH will initiate a session with CN by sending the current timestamp of 12 bits. The registration packet is encrypted using the key F_1 which involves the operation as XOR, extraction, shift and concatenation and the encrypted registration packet is obtained. CH will broadcast the encrypted packet towards CN and also send the time TCH-present to BS.

Encrypted packet is decrypted by CN with the use of same key F_1 followed by the operations split, extraction, shift and XORed. Finally T'_{reg} is obtained. If T'_{reg} matches the 8 bits from the MSB of T_{reg} stored in CN then it is considered that the message from CH is confirmed and thus it guarantees integrity.

Once all the query is registered from BS to CH, the registration response phase is developed from CH to CN. The registration response phase is completed from CN to CH and also from CH to CN. After registration the query is forwarded from CH to CN and also from CH to the BS.

Pseudocode: Query Phase

```
// Operation at BS
        BS spread its timestamp to CH
        Transmit 8 bit query
// Encryption
        8 bit query XORed with 4 bits of timestamp
        Obtain $H_E$ and its complement $H'_E$
        $H'_E$ and query are concatenated
        Encrypted query $H''_E$ obtained
// Operation at CH
        Encrypted query accepted
        $H'_E$ complemented to form $H_E$
        high weight of timestamp and orginal timestamp are compared
        message from BS is confirmed
//query registration
        CH broadcast 12 bits of timestamp
        Key $F_1$ created
        registration packet is created
        creates an encrypted registration packet
//CN operation
        Encrypted registration packet is received
        XORed with $F_1$
        registration timestamp is obtained
        if registration timestamp equals encrypted registration timestamp
        then accept
        else
        rejected
// query forwarding response phase
        CH collects the response from CN
        query response is created
//operation at BS
        receive the created query response
        check attacks is possible
        if no attack
        accept
        else
        reject
```

V. SIMULATION

The simulation is performed in MATLAB (version 7.2). for simplicity, it is assumed that the nodes are randomly deployed in the network and all nodes in the network will have the equal amount of energy.

At the time of implementation the network is deployed with 100 number of nodes and the value of malicious nodes may range from 5 to 25 also an average independent runs of 50 runs is performed.

Parameters	Value
Initial energy of node	3J
Network Area	(50X50) – (120 X120)m^2
Communication range	130 m
Sensing range	60 m

Table 1: Simulation parameters

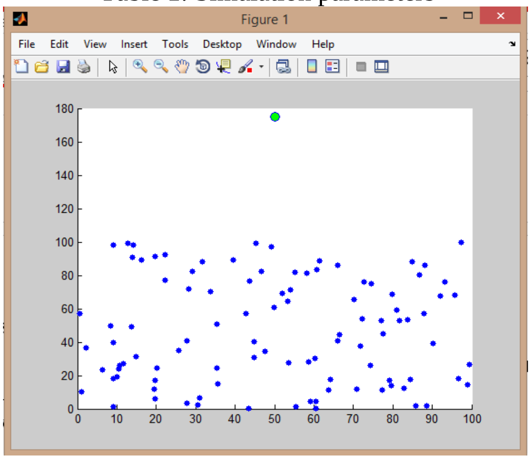
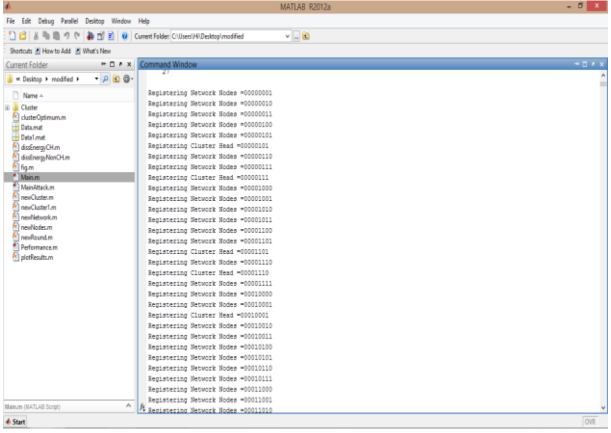


Fig. 2: Node deployment

The performances are evaluated based on the criteria as Data Freshness, Packet Delivery Ratio and the Average energy of the nodes.

Fig dpecits that the nodes are randomly deployed in the network. The x-coordinate and y-coordinate shows the location of the nodes in the yard.


MATLAB R2012a
File Edit Debug Parallel Desktop Window Help
Current Folder: C:\Users\Hi\Desktop\modified
Current Folder
Command Window

```
Registering Network Nodes =00000001
Registering Network Nodes =00000010
Registering Network Nodes =00000011
Registering Network Nodes =00000100
Registering Network Nodes =00000101
Registering Cluster Head =00000101
Registering Network Nodes =00000110
Registering Network Nodes =00000111
Registering Cluster Head =00000111
Registering Network Nodes =00001000
Registering Network Nodes =00001001
Registering Network Nodes =00001010
Registering Network Nodes =00001011
Registering Network Nodes =00001100
Registering Network Nodes =00001101
Registering Cluster Head =00001101
Registering Network Nodes =00001110
Registering Cluster Head =00001110
Registering Network Nodes =00001111
Registering Network Nodes =00010000
Registering Network Nodes =00010001
Registering Cluster Head =00010001
Registering Network Nodes =00010010
Registering Network Nodes =00010011
Registering Network Nodes =00010100
Registering Network Nodes =00010101
Registering Network Nodes =00010110
Registering Network Nodes =00010111
Registering Network Nodes =00011000
Registering Network Nodes =00011001
Registering Network Nodes =00011010
```

Fig. 3: Cluster Formation and Registration

The clusters are formed and the nodes in the network will be registered to the BS. During this process the CH is elected and the remaining nodes in the network will be assingned to their nearby CH's.

A. *Data Freshness*

Data freshness is used to specify whether the replay attack has happened or not. It is defined as the ratio of number of packets received by CH containing current data to the total number of packets sent by CN during one communication cycle.

$$data\ freshness = \frac{A}{B} * 100$$

Where A = no. of packets received by CH containing current data and B = total no.of packets sent by CN

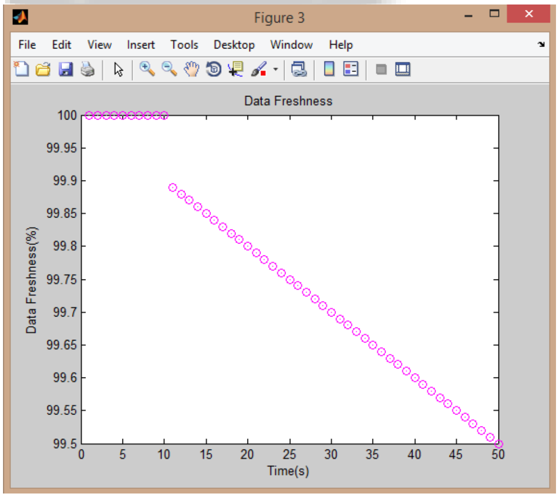


Fig. 4: Data Freshness

Fig displays the data freshness graph, the x-coordinate is labeled with the data freshness and the y-coordinate is labeled with the time. 99.9% of the data freshness is achieved.

B. *Packet Delivery Ratio*

Packet delivery ratio is used to measure the performance of network that specifies the number of packets distributed and the number of packets received in the presence of an attacker. It is defined as the ratio of number of packets received by a cluster head to the total number of packets sent towards the cluster head.

$$Packet\ Delivery\ Ratio = \frac{C}{D} * 100$$

Where C = no.of packets received by CH and D = total no.of packets send to CH.

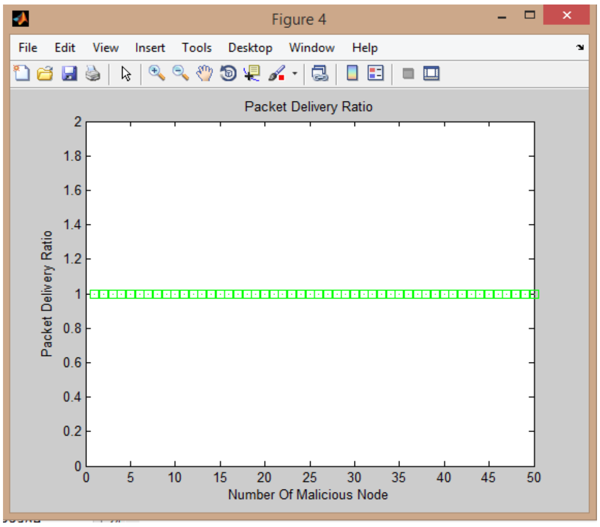


Fig. 5: Packet Delivery Ratio

Fig displays the packet delivery ratio, the x-coordinate defines the packet delivery ratio and the y-coordinate defines the number of malicious nodes. The delivered data packet have the probability value of 1.

C. *Energy*

Energy in WSN is used to determine the how much of energy is transmitted for every round of communication.

$$ET(l,d) = A\ elec * l + A\ amp * l * d^2$$

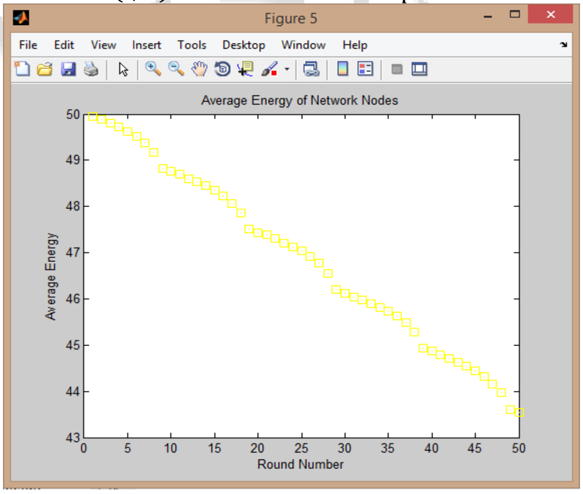


Fig. 6: Average Energy of Network Nodes

Fig displays the average energy of network nodes transmitted during the communication round. The x-coordinate specify the average energy and the y-coordinate specify the round number. The achieved energy rate will vary for every single communication.

VI. Conclusion

The presented work proposed a light weight security scheme for secure query processing in WSN. It provides security features for every step of communication to make the network robust and to protect the network from attacks.

During the communication from CH to MN, the key is neither transmitted or it is pre deployed in the nodes to eliminate the probability of gaining the transmitted key by the adversaries. Security is achieved by providing confidentiality and integrity. The performance of the model is determined by calculating authentication rate, data freshness and the packet delivery ratio and so it achieves a better results. The work is based on architecture dependent so it is likely to be extended to work in an architecture independent platform and also try to achieve the 100% integrity level.

REFERENCES

[1] Wu Y, Keally M, Zhou G, Mao W. "Traffic-aware channel assignment in wireless sensor networks". In: Proceeding of the international conference on wireless algorithms, systems and applications (WASA), LNCS-5682; 2009. p. 479–88.

[2] Ouyang Y, Le Z, Chen G, Ford J, Makedon F. "Entrapping adversaries for source protection in sensor networks". In: Proceeding of the international symposium on world of wireless, mobile and multimedia networks; 2006. p. 23–34.

[3] Vinidha, Ajay D.Vimalraj and C.Maria Antoine Pushparaj "Energy Efficient Protocol with Static Clustering (EEPSC) Comparing with Low Energy Adaptive Clustering Hierarchy (LEACH) Protocol" ISSN 2224-610X (Paper) ISSN 2225-0603 (Online), Vol.3, No.7, 2013.

[4] Nangai Abinaya S, Sudha R "A Clustering Mechanism for Energy Efficient Routing Path" IJIRCCE, Vol 2, Special Issue 1, March 2014

[5] Nitin Jain, Samir R. Das and Asis Nasipuri "A Multichannel CSMA MAC Protocol with Receiver-Based Channel Selection for MultihopWireless Networks"

[6] G. S. R. Emil Selvan, S. Sivagurunathan, P. Subathra, and S.Dina Nidhya "Mobile Ad Hoc Network Security-A Cluster based Approach"

[7] Jingbin Zhang, Gang Zhou, Chengdu Huang, Sang H. Son and John A. Stankovic "TMMAC: An Energy Efficient Multi-Channel MAC Protocol for Ad Hoc Networks"

[8] Shih-I Huang, Shiuhpyng Shieh and J. D. Tygar "Secure encrypted -data aggregation for wireless sensor networks" In Wireless Networks, 16:4, May 2010, pp. 915-927.

[9] Wendi Rabiner Heinzelman, Anantha Chandrakasan and Hari Balakrishnan "Energy-Efficient Communication Protocol forWireless Microsensor Networks" Proceedings of the 33rd Hawaii International Conference on System Sciences – 2000. Sipra Dasbit,