ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Trustworthy Based Routing In Wireless Sensor Networks

[I]Jaishankar.V, [II]Kanagachidambaresan.G.R,
[III]Mookhambika Lakshmanan, [IV]Tessia Elizabeth Mathew
[I,IV]PG Student, [II,III]Assistant Professor, CSE
[I,II,III]Dept. of Computer Science, Dhanalakshmi Srinivasan College Of Engineering, Coimbatore
[IV]Dept. of Computer Science, Rajagiri School Of Engineering and Technology, Kochi

Abstract
Providing data security in terms of confidentiality, integrity, and availability, in wireless sensor networks (WSNs) is challenging today. WSNs are exposed to many types of severe insider attacks due to node compromise. The existing security designs provide a hop-by-hop security paradigm and thus are vulnerable to such attacks. The protection of integrity and confidentiality of information and the protection from unauthorized access are important issues. A new algorithm is developed for the formation of trustworthy route from source to sink for secure routing of messages in Wireless Sensor Networks (WSNs). Execution of this algorithm at any node, gives different trusted routes to the BS with different route trusts by filtering the un-trusted nodes on the basis of trust metrics levels. The source node selects the best trustworthy route among many trusted routes given by the neighbour nodes. Based on neighbour nodes trust levels and the route trust levels of different routes given by them, the newly formed trustworthy route from source to sink will be the best trustworthy route without considering the malicious/selfish nodes. The data can be classified as top secret, private data and public data depending upon the security level. The proposed framework is favoured to classify the data based on the confidentiality level by confidentiality, integrity and availability, and then transmit the data packet through a secure path in WSN.

Keywords
Trustworthy, Confidentiality, Wireless Sensor Networks, Base Station, Integrity.

I.Introduction

A Wireless Sensor Network (WSN) is composed of autonomous devices called sensor nodes that generally have low computational power, limited data transmission and power constraints. A WSN consists of sensor nodes that capturing information from an environment, processing data and transmitting them via radio signals. WSNs are increasingly present in our days and can be found in environmental area (climatic measurements, presence of smoke), in health area (measurement of vital signs, temperature), home automation (motion sensor and image sensor) and other areas. Generally, WSNs have no fixed structure, and in many cases there is no monitoring station of sensor nodes during the operational life of the network, so a WSN must have mechanisms for self-configuration and adaptation in case of failure, inclusion or exclusion of a sensor node.

Security requirements of WSNs are similar to conventional computer networks, therefore parameters such as confidentiality, integrity, and availability must be taken into account in creation of a network environment.

Due to limitations of WSNs, not all security solutions designed for conventional computer networks can be implemented directly in WSN.A wireless sensor network (WSNs) consists of a large number of light-weight sensor nodes having limited battery life, computational capabilities, storage, and bandwidth. These low-cost sensor nodes can be deployed either randomly by dropping from an airplane or precisely using manual deployment. These sensor nodes sense a change in the environmental or a physical quantity and transmit this data to the base station, also referred to as a sink node. The sink node is usually a powerful machine like a Laptop or a Desktop. This emerging technology has been adopted by many fields as a promising solution to numerous challenges. For example WSNs is used in remote sensing, real-time trace monitoring, weather monitoring, military surveillance, health care and many other areas.

In large scale WSN, the nodes are located far from the sink and therefore use the intermediate nodes to route the data packet towards the sink.

Routing in WSNs is very important and it is distinguished from other networks due to the following characteristics:

A. IP-based Scheme

An IP-based scheme is difficult to be applied in WSNs, because of limited available resources and an extremely largescale. Unlike traditional routing protocol, in WSNs, most traffic is routed from nodes to the base station.

B. Resource Constrained

In WSNs, the nodes are resource constrained in terms of energy, storage, and computational capacity. Efficient use of resources is essential. There are mainly two types of routing techniques, single path routing and multiple path routing. Single path routing is simple and scalable, but does not efficiently satisfy the requirements of resource constrained in WSNs. It is simple because the route between the source node and the destination node can be established in a specific period of time. It is scalable because, even if the network changes from ten nodes to ten thousand nodes, the complexity and the approach to discover the path remains the same. While considering the characteristics of WSNs, single path routing is not efficient. In a single path routing, it is easy for the source node to select the intermediate data routing nodes from the same part of the network over and over again.

Multipath routing is an alternative routing technique, which selects multiple paths to deliver data from source to destination. Because of the nature of multipath routing that uses redundant paths, multipath routing can largely address the reliability, security and load balancing issues of single path routing protocols. Thus, multipath routing plays an important role in WSNs and many multipath routing protocols have been proposed in the literary of WSN. WSNs research takes an initial step to summarize all multipath routing techniques proposed in the WSN research literary. The major concern of the protocols within category A is to construct and maintain specific multipath infrastructure by

considering location and resource capabilities. Protocols which do not build any specific infrastructure and decide the next hop on the basis of its local knowledge are classified into category B. The category C protocols use variant kinds of coding schemes to fragment the data packet at the source node and then send the chunks through discovered multiple paths.

II. Related Works

There is a large number of current works, as well as efforts that are on the go, for the development of routing protocols in WSNs. Wireless Sensor Networks are heterogeneous systems containing many small devices called sensor nodes and actuators with general-purpose computing elements.

These networks will consist of hundreds or thousands of low cost, low power and self-organizing nodes which are highly distributed either inside the system or very close to it. These nodes consist of three main components-sensing, data processing and communication

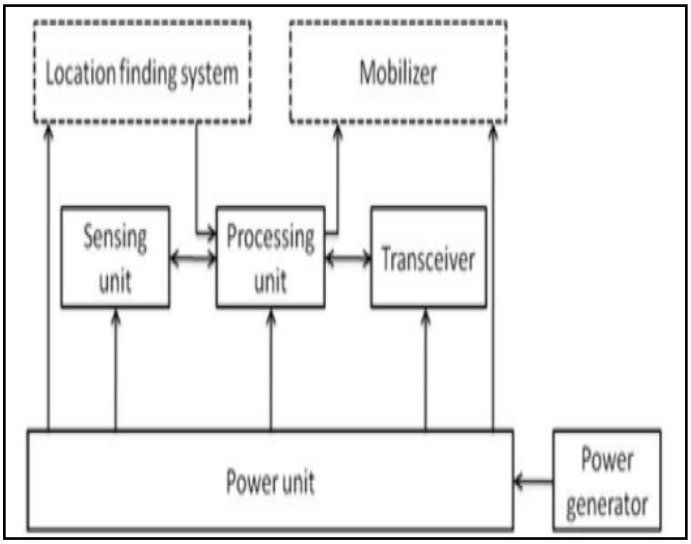


Fig. 1: Sensor node components

Data confidentiality is the most important issue in network security. Confidentiality means restricting data access to authorized personnel. The data should not be leaked across adjacent sensor networks. For this purpose, the message is sent on the channel in encrypted form. Every network with any security focus will typically address this problem first. Confidentiality is the property of protecting the content or information all users other than those intended by the legal owner of the information. In WSN the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. Confidentiality in sensor networks can be defined as: A sensor node should not reveal its data to the neighbours.Establishing and maintaining confidentiality is extremely important when node identities and keys are being distributed to establish a secure communication channel among sensor nodes. In sensor networks, the confidentiality relates to the following:

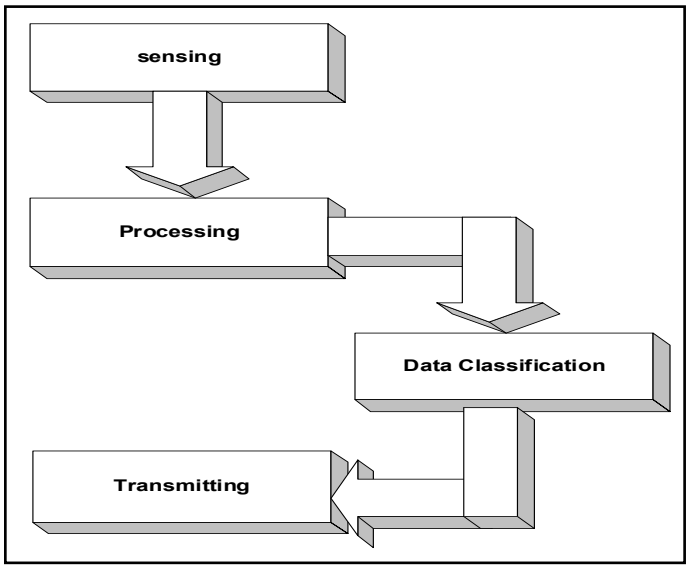
- A sensor network should not leak sensor readings to its neighbours. Especially in a military application, the data stored in the sensor node may be highly sensitive.
- In many applications nodes communicate highly sensitive data, e.g., key distribution. Therefore it is extremely important to build a secure channel in a wireless sensor network.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, thus achieving confidentiality.

Data integrity ensures that the receiver receives unaltered data in transit by any unauthorized personnel. With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transmit.

Availability ensures that the desired network services are available even in the presence of denial of service attacks. Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some approaches choose to modify the code to reuse as much code as possible. Some approaches try to make use of additional communication to achieve the same goal. What's more, some approaches force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm. But all these approaches weaken the avail-ability of a sensor and sensor network for the following reasons:

- Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
- Additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.
- A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network.

System Architecture



Due to recent technological advances, the manufacturing of small and low cost sensors became technically and economically feasible. The sensing electronics measure ambient conditions

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

related to the environment surrounding the sensor and transforms them into an electric signal. Processing such a signal reveals some properties about objects located and/or events happening in the vicinity of the sensor. A large number of these disposable sensors can be networked in many applications that require unattended operations.

III. Proposed System

Modules Description

1. Sensing Data
2. Processing
3. Data Classification
4. Trustworthy Routing and Transmission

A. Sensing Data

A Wireless Sensor Network (WSN) contain hundreds or thousands of these sensor nodes. These sensors have the ability to communicate either among each other or directly to an external base-station (BS). A greater number of sensors allows for sensing over larger geographical regions with greater accuracy .Basically , each sensor node comprises sensing, processing, transmission, mobilize, position system, and power units (some of these components are optional like the mobilize).

Sensor nodes are usually scattered in a sensor field, which is an area where the sensor nodes are deployed. Sensor nodes coordinate among themselves to produce high-quality information about the physical environment. Each sensor node bases its decisions on its mission, the information it currently has, and its knowledge of its computing, communication, and energy resources.

Each of these scattered sensor nodes has the capability to collect and route data either to other sensors or back to an external base station(s). A base-station may be a fixed node or a mobile node capable of connecting the sensor network to an existing communications infrastructure or to the Internet where a user can have access to the reported data.Networking unattended sensor nodes may have profound effect on the efficiency of many military and civil applications such as target field imaging, intrusion detection, weather monitoring, security and tactical surveillance, distributed computing, detecting ambient conditions such as temperature, movement, sound, light, or the presence of certain objects, inventory control, and disaster management.

Deployment of sensor network in these applications can be in random fashion (e.g., dropped from an airplane) or can be planted manually. For example, in a disaster management application, a large number of sensors can be dropped from a helicopter. Networking these sensors can assist rescue operations by locating survivors, identifying risky areas, and making the rescue team more aware of the overall situation in the disaster area. In the past few years, an intensive research that addresses the potential of collaboration among sensors in data gathering and processing and in the coordination and management of the sensing activity were conducted. However, sensor nodes are constrained in energy supply and bandwidth.

Thus, innovative techniques that eliminate energy in that would shorten the lifetime of the network are highly required. Such constraints combined with a typical deployment of large number of sensor nodes pose manychallenges to the design and management of WSNs and necessiti ate energy-awareness at all layers of the networking protocol stack. For example, at the network layer, it is highly desirable to methods for energy efficient route discovery and relaying of data from the sensor nodes to the BS so that the lifetimeof the network is maximized.

B. Processing

Since the sensor node is expected to communicate, toprocess and to gather sensor data, sensor nodes must haveprocessing units. The central processing unit of a sensor node determines to a large degree both the energyconsumption as well as the computational capabilities of sensor node. Many different types of CPUs can be integrated into a sensor node and there are a large number of commercially available microcontrollers, microprocessors and field-programmable gate arrays (FPGAs), which allows a big flexibility for CPU implementations.

C. Data Classification

For the secure routing of data through a WSN first we need to classify the data according to the confidentiality level of data and then route the data through a secure channel. The confidentiality level of a data mainly depends on three factors that are Confidentiality, Integrity and Availability (CIA) of data. The data can be classified as top secret, private data and public data depending upon these factors.

The top secret data are the data with high confidentiality. The private data are those data with medium level of confidentiality. Public data are free to access and they have very low confidentiality level. The classification of data based on the confidentiality, integrity and availability can be represented as a matrix.

Matrix for data classification

	Confidentiality	Integrity	Availability
Top secret	1	1	1
Private	0	1	1
Public	0	0	1

Algorithm for data classification

Algorithm for data classification

Input: C← confidentiality, a← availability, i← integrity

Output: D← Data classification

```
Begin process
    If (c ←true)
      If (i ←true)
        If (a ←true)
            D=C_H
```

```
        Else
            Deny
    If (i ←true)
        If (a ←true)
                D=CM
        Else
            Deny
    If (a ←true)
                D=CL
        Else
            Deny
End process
```

Highly confidential ←C_H, Medium confidential (private) ← C_M, Low confidential (public) ← C_L

Data confidentiality is the most important issue in network security. Confidentiality means restricting data access to authorized personnel. The data should not be leaked across adjacent sensor networks. For this purpose, the message is sent on the channel in encrypted form.

Every network with any security focus will typically address this problem first. Confidentiality is the property of protecting the content or information all users other than those intended by the legal owner of the information. In WSN the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential. This is the most important issue in network security. Confidentiality in sensor networks can be defined as: A sensor node should not reveal its data to the neighbors. For example, in a sensitive military application where an adversary has injected some malicious nodes into the network, confidentiality will prevent them from gaining access to information regarding other nodes.

Establishing and maintaining confidentiality is extremely important when node identities and keys are being distributed to establish a secure communication channel among sensor nodes. In sensor networks, the confidentiality relates to the following:

- A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.
- In many applications nodes communicate highly sensitive data, e.g., key distribution.Therefore it is extremely important to build a secure channel in a wireless sensor network.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, thus achieving confidentiality.

Data integrity ensures that the receiver receives unaltered data in transit by any unauthorized personnel. With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

Availability ensures that the desired network services are available even in the presence of denial of service attacks. Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some approaches choose to modify the code to reuse as much code as possible.

Some approaches try to make use of additional communication to achieve the same goal. What's more, some approaches force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm.

But all these approaches weaken the avail-ability of a sensor and sensor network for the following reasons:

- Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
- Additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.
- A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the whole network.

D. Trustworthy Routing and Transmission

Once the data has been classified then the next step is to route the data according to the confidentiality level of data through secure hops. In a cluster based architecture of WSN there will be a number of clusters and each cluster will have one cluster head CH and a number of cluster clients CC.

If one CC wants to send a data to another CC, first it is need to find out the path according to the level of confidentiality for performing the hop. The one cluster client can send data to another cluster client in different or same cluster. The path is finding out by calculating the trust value of each mote through which the data packet is transferred using a hop by hop communication.

If the data is top secret then the trusted value of each node should be between 1 and 0.5 and if the data confidentiality level is private then the value will be between 0.5 and 0. If the data is public then it has very low confidentiality level then the data can be transferred through the motes which have trust value between 0and -1.If these conditions are satisfied then the communication will be successful and can provide different level of security based on type of each data.

To secure multi-hop routing in WSNs against intruders exploiting the replay of routing information, we propose trustbased routing framework for WSNs. It incorporates the trustworthiness of nodes into routing decisions and allows a node to circumvent an adversary misdirecting considerable traffic with a forged identity attained through replaying.

Algorithm for Routing and Transmission

Algorithm for routing

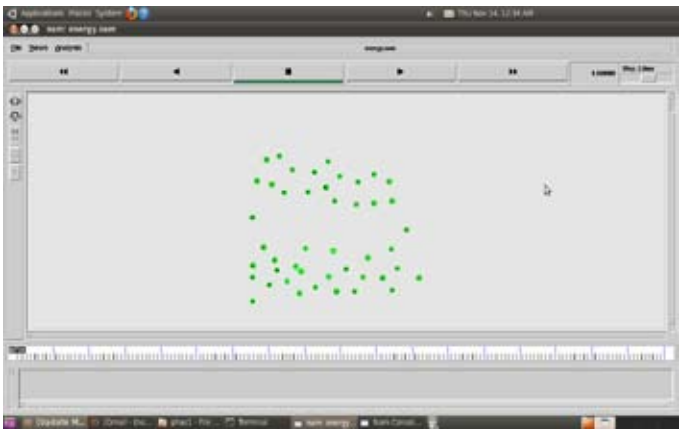
C_S← cluster client sending request
C_{H0}← Cluster head of CS
C_{Hi}← Other cluster head
C_R← Cluster client receiving request
D← data classification
C_H← highly confidential
C_M← Medium confidential (private)
C_L← Less confidential (public)

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

1. communicate ($C_S \rightarrow C_{H0}$)
2. for each C_{Hi}
   calculate trust value O_i
   if ($D \leftarrow C_H$)
   if($0.5<O_i<1$)
   communicate ($C_{H0} \rightarrow C_{Hi}$)
   check for C_R
   if found
   communicate ($C_{Hi} \rightarrow C_R$)
   Exit loop
   else
   Assign $C_{H0} \leftarrow C_{Hi}$ and
   repeat step 2
   else
   cancel the hop
   if ($D \leftarrow C_M$)
   if($0<O_i<0.5$)
   communicate ($C_{H0} \rightarrow C_{Hi}$)
   check for C_R
   if found
   communicate ($C_{Hi} \rightarrow C_R$)
   Exit loop
   else
   Assign $C_{H0} \leftarrow C_{Hi}$ and
   repeat step 2
   else
   cancel the hop
   if ($D \leftarrow C_L$)
   if($-1<O_i<0$)
   communicate ($C_{H0} \rightarrow C_{Hi}$)
   check for C_R
   if found
   communicate ($C_{Hi} \rightarrow C_R$)
   Exit loop
   else
   Assign $C_{H0} \leftarrow C_{Hi}$ and
   repeat step 2
   else
   cancel the hop
3. Stop

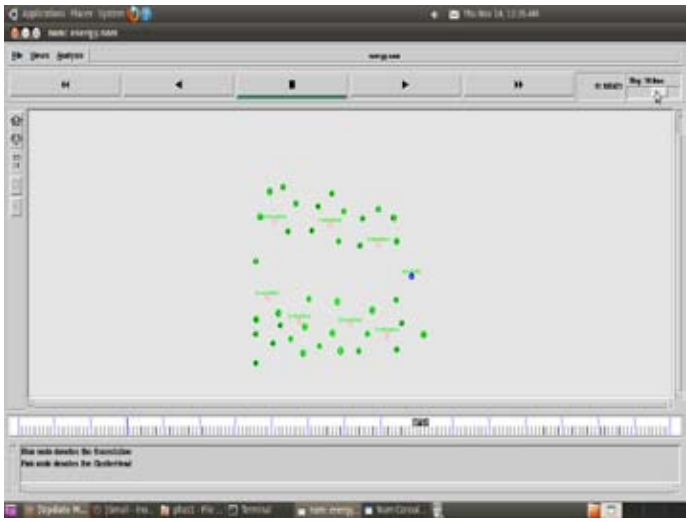
IV. Results And Discussions

1. Sensing data



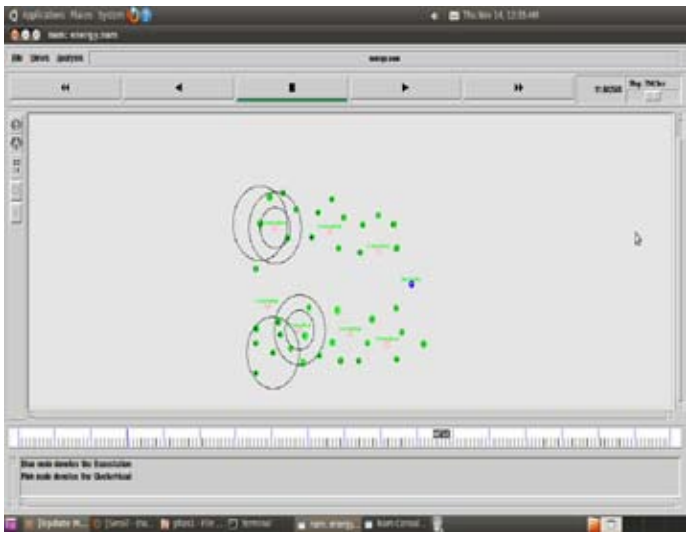
Wireless Sensor Network (WSN) is a wireless network consisting of small nodes with sensing, computation, and wireless communications capabilities (Karaki, 2004). As wireless sensor networks consist of hundreds to thousands of low-power multi functioning sensor nodes, operating in an unattended environment, with limited computational and sensing capabilities. Sensor nodes are equipped with small, often irreplaceable batteries with limited power capacity. WSN consist of hundreds or thousands of small, cheap, battery-driven, spread-out nodes bearing a wireless modem to accomplish a monitoring or control task jointly. Each sensor collects data from the monitored area (such as temperature, sound, vibration, pressure, motion or pollutants).

2. Cluster Head Selection



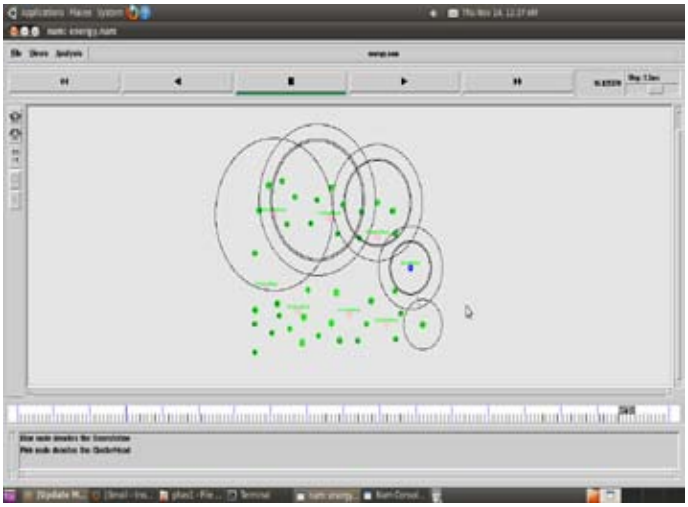
Cluster Heads(CHs) collects the data from respective cluster's nodes and forward the aggregated data to base station. A major challenge in WSNs is to select appropriate cluster heads. Selection of CHs using three criteria including residual energy, number of neighbors, and the distance from the base station of the nodes. The simulation results demonstrate that this approach is more effective in prolonging the network lifetime than the distributed hierarchical agglomerative clustering (DHAC) protocol in homogeneous environments.

3. Processing the data



It simply processing the data at the front-end of sensor node and only transmits the abnormal data to largely compress the source data. In order to process some data from the front-end, testing center of the back-end adopts the cluster analysis algorithm based on genetic algorithm.

4. Data Classification

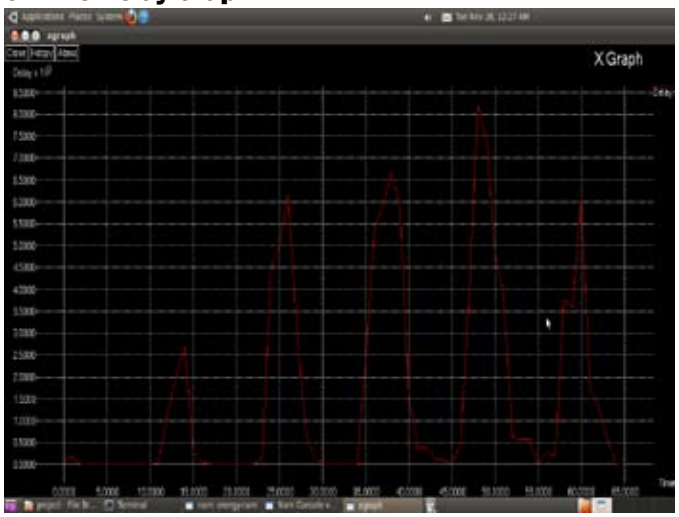


In addition to sensing and processing, providing a secure data transmission and efficient data classification is a crucial issue in sensor networks in order to obtain accurate data and reduce the communication overhead. Hence, a fast, accurate and efficient classification algorithm will help to decrease the number of data transmitted over the network. For that classification based on CIA is proposed.

5. Data Transmission and Trustworthy Routing

To secure multi-hop routing in WSNs against intruders exploiting the replay of routing information, we propose trustbased routing framework for WSNs. It incorporates the trustworthiness of nodes into routing decisions and allows a node to circumvent an adversary misdirecting considerable traffic with a forged identity attained through replaying. Both our empirical and simulated experimental results indicate that satisfactorily performs routing and is re-silient against attacks by exploiting the replay of routing information.

6. Time Delay Graph



WSNs are used in defense field where less time delay and life of sensors are most important because the life of soldier are depends on fast information transmission. Hence energy and time delay are very scarce resources for such sensor systems and has to be managed wisely in order to extend the life of the sensors and minimizing time delay for the duration of a particular mission.

V. Conclusions

The security of data transmissions from these devices should be improved in a preventative manner to avoid possible attacks in secure label-switching routing protocol for wireless sensor networks, called Trust Based Routing Protocols in WSNs, which is an efficient reactive routing protocol for wireless sensor networks. It specifies how to provide better routing path for transmitting the packets from source from destination and presented a over view of Trust aware routing protocol for secure routing in Wireless sensor Networks, and modules involved in that to improve the performance for designing how the modules are selecting the better route for transmitting packets. A trust-aware routing framework for WSNs, to secure multi-hop routing in WSNs against intruders exploiting the replay of routing information is developed with the idea of trust management, it enables a node to keep track of the trustworthiness of its neighbors and thus to select a reliable route. At this stage, the first part of the algorithm, i.e. formation of trusted paths between benevolent nodes is simulated to develop a new algorithms to detect the different attacks easily, mange trust relations accordingly and it shall also be able to manage other dynamic aspect of trust i.e. trust revocation. To the best of our knowledge, our work is the first in the field to introduce a complete trust evaluation of sensor data during their life cycle. The pro-posed implementation of our trust model then address draw-backs introduced by existing approaches: heterogeneity, the fact that they only consider origin or value in trust evaluation, and the lack of condense determination in fusion of information.

References

[1] *Hong-Chi Shih and Jeng-Shyang Pan, "Fault Node Recovery Algorithm for a Wireless Sensor Network," ieee sensors journal, vol. 13, no. 7, july 2013.*

[2] *I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cyirci, "Wireless Sensor Networks: A Survey," Computer Networks, vol. 38, no. 4, pp. 393-422, Mar. 2002.*

[3] *R.B. Araujo, and L. Villas, "Optimal Route Selection for*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Highly Dynamic Wireless Sensor and Actor Networks Environment," Proc. 10th ACM Symp. Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWiM '07),pp. 21-27, 2007.

[4] G. Anastasi, M. Conti, M. Francesco, and A. Passarella, "Energy Conservation in Wireless Sensor Networks: A Survey,"Ad Hoc Networks,vol. 7, no. 3, pp. 537-568, http://dx.doi.org/10.1016/ j.adhoc.2008.06.003, May 2009

[5] A. Boukerche E. M. Royer and C. K. Toh, "A review of current routing protocols for ad-hoc mobile networks," IEEE Personal Commun., vol. 6, no. 2, pp. 46–55, Apr. 1999.

[6] J. A. Carballido, I. Ponzoni, and N. B. Brignole, "CGD-GA: A graph-based genetic algorithm for sensor network design,"Inf. Sci., vol. 177, no. 22, pp. 5091–5102, 2007.

[7] S. C. Chu ,H. C. Shih, , J. Roddick, J. H. Ho, B. Y. Liao, and J. S. Pan, "A reduce identical event transmission algorithm for wireless sensor networks," inProc. 3rd Int. Conf. Intell. Human Comput.Interact., 2011, pp. 147–154.

[8] F. C. Chang and H. C. Huang, "A refactoring method for cache-efficient swarm intelligence algorithms," Inf. Sci., vol. 192, no. 1, pp. 39–49,Jun. 2012.

[9] S. Corson and J. Macker,Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations.NewYork,NY, USA: ACM, 1999.

[10] D. Estrin, C. Intanagonwiwat, R. Govindan, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking,"IEEE/ACM Trans. Netw., vol. 11, no. 1, pp. 2–16, Feb. 2003.

[11] M. Gen and R. Cheng, Genetic Algorithms and Engineering Design. New York, NY, USA: Wiley, 1997

[12] J.H.Ho, H.C.Shih, B. Y.Liao, and J.S.Pan, "Grade diffu-sion algorithm," in Proc. 2nd Int. Conf. Eng. Technol. Innov., 2012, pp. 2064–2068.

[13] B.Y. Liao, and S. C. Chu, "A ladder diffusion algorithm using ant colony optimization for wireless sensor networks," Inf. Sci., vol. 192, pp. 204–212, Jun. 2012.

[14] J. Pan, Y. Hou, L. Cai, Y. Shi, and X. Shen, "Topology control for wireless sensor networks," inProc. 9th ACM Int. Conf. Mobile Comput.Netw., 2003, pp. 286–299.

[15] K. Romer and F. Mattern, "The Design Space of Wireless Sensor Networks,"IEEE Wireless Comm.,vol. 11, no. 6, pp. 54-61, Dec. 2004.

[16] S. Ramasubramanina and O. Younis, M. Krunz "Node Clustering in Wireless Sensor Networks: Recent Developments and Deploy-mentChallenges,"IEEE Network, vol. 20, no. 3, pp. 20-25, Dec. 2006.

[17] S. Solarium, Q. Xu, and A. Zomaya, "An Energy-Efficient Self-Organization Protocol for Wireless Sensor Networks,"Proc. IEEE Intelligent Sensors, Sensor Networks and Information Processing Conf. (ISSNIP),pp. 55-60, Dec. 2004.

[18] X. W. Wang T. H. Liu, S. C. Yi "A fault management protocol for low-energy and efficient wireless sensor networks,"J. Inf. Hiding Multimedia Signal Process., vol. 4, no. 1, pp. 34–45, 2013.

[19] C. H. Wu and T. P. Hong "An improved weighted clustering algorithm for determination of application nodes in heterogeneous sensor networks," J. Inf. Hiding Multimedia Signal Process., vol. 2, no. 2, pp. 173–184,2011.