International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 4, Issue 4, April 2015

INTRUSION DETECTION FOR DEPENDABLE TRUST SYSTEM IN WIRELESS SENSOR NETWORKS WITHOUT PACKETLOSS

M.SUGANYA,

ME student, sri shakthi institute of engg and technology

S.AJANTHA,

ME student ,sri shakthi institute of engg and technology,

ABSTRACT:

The security and minimum energy consumption are the major requirement in clustered wireless sensor networks (WSN).Existing trust system in WSNs are capable in satisfying these needs because of their maximum overhead and minimum dependability. In lightweight dependable trust system (LDTS) in WSNs, which follow clustering algorithm. Initially, trust decision algorithm is proposed based on node identities, which is suitable for such WSNs which has energy saving capability. Leach is the efficient technique to reduce the power consumption. It also increases the level of security. By using LEACH protocol some as watch dogs nodes and some changes is needed for intrusion detection .And one node is considered as cluster head (CHs) through the cluster head packet transferring is done. Based on trust values packet is transmitted. Through this approach security level and efficiency are increased with low energy consumption.

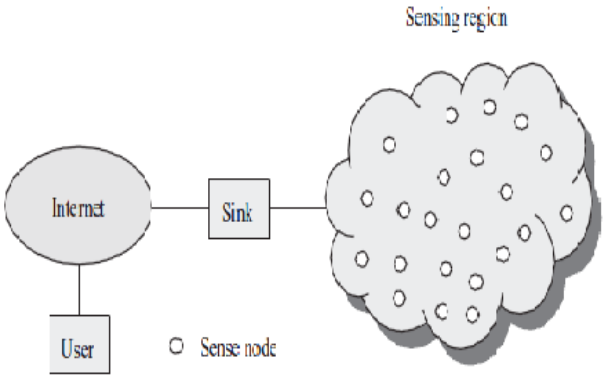
Keywords: clustering algorithm-one node as cluster head-trust values-secure transmission

1.INTRODUCTION

A collection of nodes grouped to form a network which follows a clustering algorithm. Each clustered group has a common single source node .It will send the response to the clustered head in each cluster. A Wireless Sensor Network (WSN) is distributed sensors for

measuring any changes in climatic conditions and to cooperatively pass their data through the network to the final destination. The networks with two way communication are proceeded now which controls the sensors also. Wireless sensor networks having applications in all the fields such as army, military communications and in many other fields.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Sensors includes microcontroller; transmitter and receiver .The microcontroller is interfaced with a interfacing cable. Power supply is given by the battery to the system. Sensors are of different in sizes and in shapes, although functioning "motes" of genuine microscopic dimensions have yet to be created. The manufacturing cost varies in few hundred depending on the application usage. It mainly depends on the memory usage and efficiency. The t WSNs can switch over from simple star network to an advanced multi-hop



network. The routing operation is performed when the network is connected.

Figure 1.1: Architecture of WSNs

Wireless sensor networks are classified into two type's flat architecture and hierarchical. Flat Architecture –each node plays the same role in performing sensing task and all sensor nodes are peers. Hierarchical Architecture –sensor nodes are organized clusters, where the cluster members send their data to the sink.

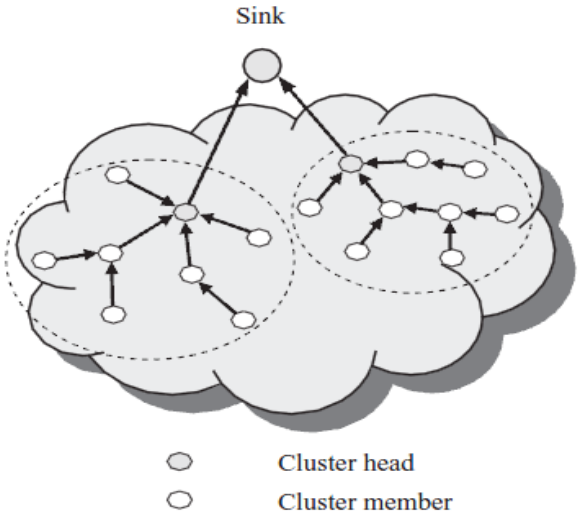


Figure1.2: Multi-hop Clustering (Hierarchal Architecture)

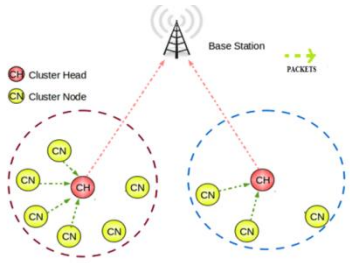
2. RELATED WORK:

Mohammed Reza Manije keshtgary Mohammed Rafi [1] proposed a system to increase the level of security with minimum power consumption. It does not detect the environment signals.Abdel mounaam Rezgui [2] proposed, RACER uses an effective service-aware routing approach that aggressively reduces downstream traffic (from the sink to the Time network's nodes) by translating service profiles into efficient paths for queries. Adaptive task selection (ATS) algorithm is used. Y.Sun Z.Hank R.Liu [3] proposed a system having to establishing trust in a clustered environment to enable the CH to detect faulty node in cluster.G .ZhanW.Shi J .Deng [4] proposed a trust system-to serve large number of resource constrained nodes in terms of additional overhead. Huang Lu [5] secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed randomly. We implement a system of having highest efficiency and security. By using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. Raquel Lacuesta, Jaime Lloret [6] proposed system to secure protocol for spontaneous wireless ad hoc networks which uses a hybrid symmetric/ asymmetric scheme and the trust between users in order to exchange the initial data and to exchange the secret keys that will be used to encrypt the data. Fenye Bao [7] proposed a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs) to effectively deal with selfish or malicious. For trust-based intrusion detection, we discover that here exists an optimal trust threshold for minimizing false positives and false negatives. Kejie Lu [8] proposed a heterogeneity features in design of a good distributed key management scheme has become an important issue. It proposes a unified framework for distributed key management schemes in heterogeneous wireless sensor networks. Zhenghao Zhang [9] proposed a two-layered heterogeneous sensor network has two types of nodes are deployed: the basic sensor nodes and the cluster head nodes. Generally sensor nodes require single power supply when nodes are connected in cluster they are in need of many power supplies for each node. Run fang Zhou [10] proposed a power trust system dynamically selects small number of power nodes that are most reputable using a distributed ranking mechanism. Power Trust significantly improves in global reputation accuracy and aggregation speed.

3. PROPOSED WORK:

Initially we made a reference study of trust systems in WSNs for better efficiency and security. The key features are as follows:

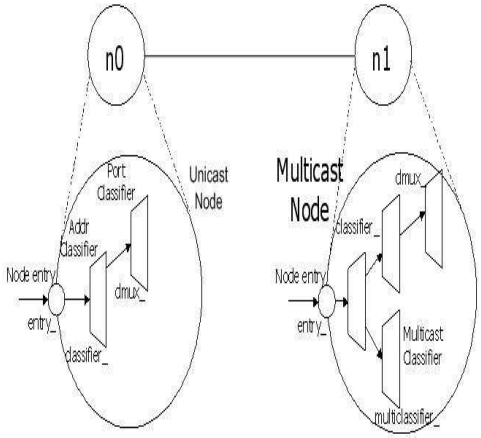
1. Based on the trust value cluster head is chosen and cluster member is controlled and directed by the clustered head.
2. Based on dependability condition the data forwarding and clustering conditions are performed by reducing faulty nodes.



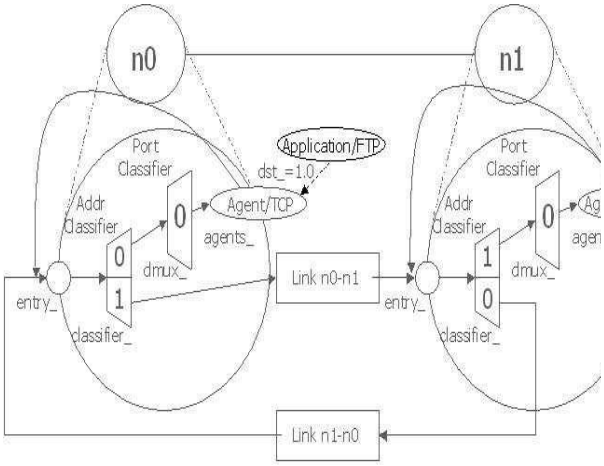
When the cluster head is chosen it sends a indication message to the source node based on trust values. Then the source node send a notification message to the clustered head to control the cluster member .Threshold value is calculated based on transmission failure in one cluster to the transmission failure in overall clusters.

3.1.NETWORK MODEL:

Our idea is to create trust based system with minimum packet loss having high efficiency and minimum aggregation time and it transmits in an effective manner. Base stations can choose the clustered head to lead the cluster member for transmitting the packets with minimum packet loss. In each cluster there will be a cluster head and a cluster member with one watch dog node. It supervises the respective cluster having to transfer the packets in secured manner. Nodes can be set in clustered format for transferring packets. Nodes having the address field a data field .when transferring data it verifies the destination field for to reach destination



3.1.1: Network Archietecture



. **3.1.2: NODE ARCHIETECTURE**

3.2. TRUST BASED SYSTEM:

In light weight dependable trust system trust values are calculated for transferring packets. Based on high trust value the packet transmission is done .Following the condition all the clusters having to made transmission based on the trust value .The cluster members controlled by the cluster head. The cluster heads are controlled by the source node. During transmission the faulty nodes which cannot have trust values are not considered for transmission. The data cannot be delivered. Energy is the scarcest resource of WSN nodes, and it determines whether the multi-hop communication network is suited for all conditions. For this reasons the following issues to be maintained:

- Lifetime maximization
- Robustness and fault tolerance
- Self-configuration

4.INTRUSION DETECTION:

The packet is transferred from source node to cluster member. When the node is coming from the next cluster it is termed as internal intruder. When the node is coming from the environment it is termed as external intruder. Both are indicated as in different format. During the transmission, because of intruder packets are lossed. By using light weight dependable trust system packet losses get reduced. It detects the attacks also in data forwarding.

4.1. ATTACKS IN DATA FORWARDING:

Sometimes intruder node as a regular node or CH doesn't send messages to related CH or BS and it drops the message or sends it to another malicious node or network. It can detect these types of attacks by checking the packet destination and CH activities and communications.

4.2. SECURITY IN SYSTEM:

During transmission there is reduction in packet loss and data efficiency with minimal over head. Generally clustered wireless sensor networks having high level of security. Most of the papers described about the security at lower level.

By using Low energy Adaptive Clustering Hierarchy (LEACH) we

achieve a high security level with minimum energy consumption. The packets are transferred in highly secure manner. The algorithm as follows:

ALGORITHM:

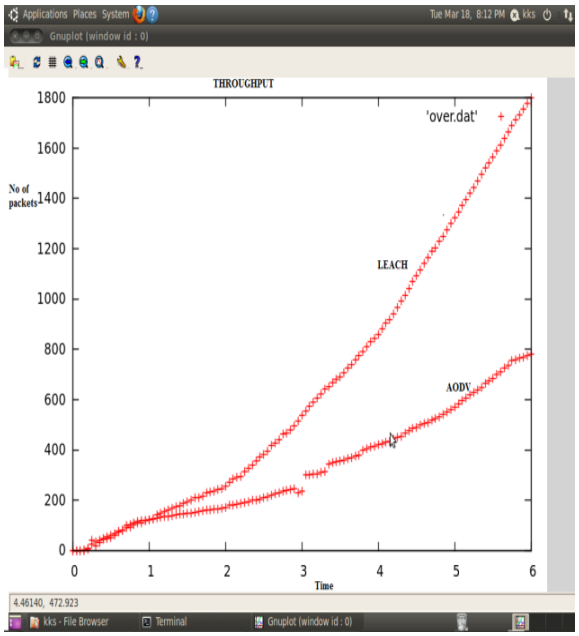
1. for all cluster members in cluster
2. If transmission failure in cluster>overall transmission failure
3. Intruder indication
4. Else
5. Packet transmission
6. End
7. End

5. PERFORMANCE ANALYSIS:

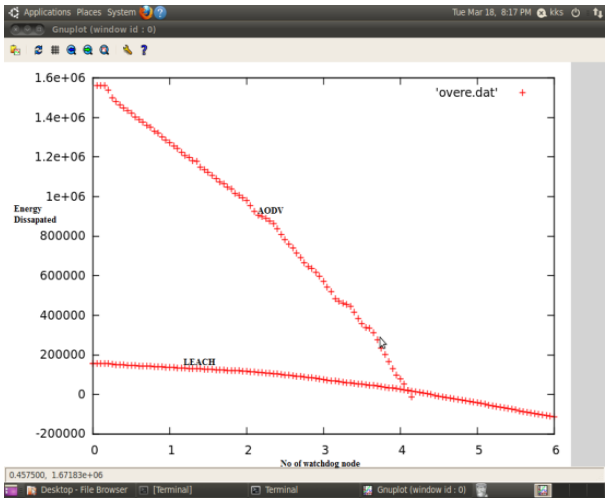
In many other papers they reached the efficiency of about 2-3%.By using LEACH we attain an efficiency of about 80%.It maintains the high efficiency with minimum energy consumption compared to other protocol. We have compared the LEACH protocol with other protocol as:

Throughput analyses have been examined for using leach protocol is increased more than the other protocol. And it consumes less energy for transmission of packets .

5.1.THROUGHPUT



5.2.ENERGY DISSIPATION



CONCLUSION AND FUTURE WORK:

Leach is an efficient technique it can be combined with any other applications. It is more useful in real time applications also. It maintains high

security with minimum packet loss. This protocol can detect the faulty node compared to any other protocol. It can be used for monitoring purposes also. By using LEACH protocol it occupies minimum memory adaptation. In future extension we can increase the efficiency percentage higher than the proposed system.

REFERENCES

1. Sohail abbas "light weight Sybil attack detection in manets"

2. Yenumula b. reddy "trust-based approach in wireless sensor networks using an agent to each cluster" international journal of security, privacy and trust management (ijsptm), vol.1, no.1, February 2012

3. Pedro b. velloso, rafael p. laufer, daniel de o. cunha, otto carlos m. b. duarte, and guy pujolle "trust management in mobile ad hoc networks using a scalable maturity-based model" ieee transactions on network September 2010

4. Dezun dong, student member, ieee computer society, xiangke liao, yunhao liu, "edge self-monitoring for wireless sensor networks"

5. Dali wei, member, ieee "an energy-efficient clustering solution for wireless sensor networks" ieee transactions on wireless .

6. X. Li, f. Zhou, and x. yang, "scalable feedback aggregating (sfa) overlay for large-scale p2p trust management" 2012.

7. Fenye bao,ing-ray chen, moonjeong chang, and jin-hee cho "hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection" ieee transactions on network , June 2012

8. Daojing he, student member,ieee "security analysis and improvement of a secure and distributed reprogramming protocol for wireless sensor networks" November 2013

9. Huang lu, student member, ieee , jie li, senior member, IEEE ,mohsen guizani, fellow, ieee "secure and efficient data transmission for cluster-based wireless sensor networks" journal 2012

10. G. Zhan, "design and implementation of trust aware routing framework for wireless sensor networks"

