Secure Multicast Scheme in Cluster Based Wireless Sensor Network

Manjunath CR[1] Maria Theresa Hoover[2], Sushma J[3], Sindhu Anand[4]
[1,2,3,4]Department of Computer Science and Engineering
School of Engineering and Technology
Jain University

***Abstract* – Wireless Sensor Networks (WSNs) are employed in numerous applications in different areas including military, ecology, and health; for example, to control of important information like the personnel position in a building, as a result, WSNs need security. Using multicast technology can significantly reduce energy consumption and prolong the life time of nodes in query-based wireless sensor networks (WSNs). Existing multicast protocols for WSNs mainly focus on covering multicast scope zone effectively, and assume secure communication between all nodes. A new efficient cluster based multicast tree (CBMT) algorithm for secure multicast Communication, in which source node uses Multicast version of Destination Sequenced Distance Vector(MDSDV) routing protocol to collects its 1 hop neighbours to form cluster and each node which have child node is elected as the Local controllers of the created clusters. It also tolerates the faults that causes due to failure of nodes.**

Index terms – CBMT(cluster based Multicast tree) cluster techniques, multicasting,security, WSN.

I.INTRODUCTION

wireless sensor network (WSN) consists of large number of sensor nodes. Each sensor node capable of sensing , data processing, computing, wireless communicating and monitoring object of interest or environmental conditions such as temperature ,sound, embedded processing, humidity, pressure, light intensity. As the technology of wireless sensor networks matures are used in numerous applications and emerging as an area of active research. Since Sensor node can be deployed in environmental monitoring, medical care, and home appliance management. It can be attacked during data transmission, It is important to provide secure communications between sensor nodes and base stations or Vice versa. Security should be considered because most of sensor networks possess various mission-critical tasks and hence WSN need security. [1][3][5][6][9][10][19]

II.SECURITY GOALS, SCHEME AND STRATEGY:

A. Security goals:

The security goals for the sensor nodes, as following:

Confidentiality: Data must be protected from being captured by any data adversaries.

Authentication: Need to know if the messages are from the node it claims to be from, determining the reliability of message's origin

Integrity: It refers to the ability to confirm the data must not been altered or changed between transmission due to environment

Availability: The network should not fail frequently

B. Security Scheme:

The security requirements of a wireless sensor network can be classified as follows[6-9,19]:

Data Authentication: Data authentication is fundamental for various applications in sensor networks and make sure that the data used in decision-making originate from the correct source is initiated from the exact source.

Data Confidentiality: Confidentiality means keeping information hidden from unauthorized party.i.eNodes should not reveal any data to unintended recipients.

Data Integrity: Data should not be changed between integrity transmissions due to the environment and make sure that any received message has not been modified sent by unauthorized parties.

Availability: Determine if a node has the ability to use the resources and the network is available for the messages making sure that the network should not fail frequently

Data Freshness: Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages.

C. Security Strategy:

The strategy plays major role in security[8], strategy can be divided into the following several parts: node and components, connections, transmission.

Node and components: Node has two attributes: own identity and groups' identity. Own identity value can determine only one node in key establishment process, while group identity value can determine only a group.

Connection: A pair of node has multiple connection path, Direction that describes the connection path can be symmetrical or non-symmetric connection, symmetrical connection nodes can be said to be bi-direction transmission, which can make the sender and also can be the receiver; Asymmetric connection said that the direction of transmission is unique; a node only can be as the sender or recipient. Trust represents the credibility when a node completes the transmission not be captured.

Transmission: Transmission is described by brisk index which is a number between 0 and 1,the higher index the more important the information.

There are two types of techniques used to transfer the data from source to destination: Unicast routing Multicast routing

Unicast is the transferring of data from 1 node to other that is from single source to single destination and Multicast routing, which refers to the transmission of the same data to several destinations. Research shows that multicast in wireless sensor networks has more importance. It reduces the number of packet transmission, optimizes the bandwidth consumption and save the node energy. Moreover, multicast can be useful for the next generation Internet, which will integrate WSNs [20]

To prolong the life time of WSN net with limited energy resources, Multicast can better meet the requirements of network resources having the high bandwidth utilization and effective mechanisms to save energy, Multicast packets can be transmitted efficiently to reduce energy consumption effectively. However, the widely used of multicast technology in traditional wireless networks have too much difference with Wireless sensor network, such as MAODV(multicast adhoc on-demand distance vector(MAODV)),ODMRP(On-Demand Multicast Routing Protocol) and AM (adhoc multicasting) Route multicast routing protocols which have been proposed by the mobile Ad hoc networks[21]. Ad hoc network [22]is a group of computers that based on no infrastructure tries to communicate with each other. Ad -hoc networks based on their special case of usages like in battle field or relief and rescue projects; and constrains or problems with them, like battery power constrain or moving . Problem have been turned to a complex and important field.

III. MULTICASTING IN WSN

There [1][15] is a need for different methods and techniques for secure path formation. For a secure transmission, broadcasting uses the leaf nodes which are assigned keys based on all forward nodes above them. Secure multicasting scheme considers the benefits of key management techniques; the root to key management is the key distribution centre which uses a logical key. The Multicasting system provides a secure communication mechanism to ensure the data security, integrity and verifiability. Moreover, it can be justified against security attacks and known routing attacks. There are various schemes that can be incorporated to form a secure transmission path are through key management techniques or providing security to the layers or to the data that has to be transmitted. Multicast is the communication paradigm of one-to many or many-to-many, based on defined groups and constituted by members, whose interest is to receive/share the same information for a specific application. A multicast group can also have one or more senders. Multicasting in WSNs evaluates its real impact and comparing it with the conventional unicast solutions. The multicast requirement over WSNs is based on the application nature.

A. Secure Multicasting

In [12] contrast to the traditional point-to-point communication on the internet network, the major communication pattern of WSNs is multicasting. Secure multicasting pattern: while considering the benefits of a logical key hierarchy, a directed diffusion based multicast technique for WSNs. The root of key management is the key distribution centre, while the individual sensor nodes make up the leaves. Mechanisms for sensor nodes are provided by this technique by joining and leaving groups where the key hierarchy is used to effectively re-key all the nodes within the leaving nodes.

Multicast path is based on effective tree construction and hierarchical network topology in a single framework. Such integration allows the system to be optimized in terms of energy efficiency, reducing the overhead. Secure Multicast system provides a secure communication mechanism to ensure the data security, integrity and verifiability. Moreover, it can be justified against security attacks and known routing attacks.

IV. KEY MANAGEMENT AND KEY DISTRIBUTION

A. Key Management:

Key Management is the most important issue[10] in the security of Wireless Sensor Networks. It helps in maintaining the confidentiality of secret information from unauthorized users. Sometimes, it is also useful for verifying the integrity of exchanged messages and the authenticity of the sender .Since most of the public key cryptographic mechanisms are computationally intensive, most of the research studies for WSNs focus on use of symmetric key cryptographic techniques.

Key [7] [19] management is one of the most important issues of any secure communication. With the increasing demand for the transmission security in wireless sensor networks, the key management can be done in two methods, providing session key to individual nodes and providing key management to group nodes, before exchanging data securely, encryption keys must be established among sensor nodes. Key usage for secure data transmission, it does not specify how to exchange keys securely. Besides the link layer, upper layers such as the network and application layers also must exchange keys securely. This is a challenging problem because there are many stringent requirements for key management, and the resources available to implement such processes are highly constrained. Many security-critical applications depend on key management processes to operate but also demand a high level of fault tolerance when a node is compromised.

Key distribution refers to the distribution of multiple keys among the sensor nodes. After deployment, each node must broadcast the key's ID number within its communication range to find out the nodes sharing the same key. Therefore, a secure communication can be established as long as there is at least one key being shared. If there is no shared key between two nodes, the link has to be established through two or more key paths.

B. Key Distribution schemes

The [19] three simplest keying models that are used to compare the different relationships between the WSN security and operational requirements are network keying, pairwise keying, and group keying.

Network keying model: It is simple, easy to manage, and uses very little resources. This model allows easy collaboration of nodes; neighbouring nodes can read and interpret each other's data, satisfying the self organization and accessibility requirements. Model has advantage in terms of scalability and flexibility over the other two schemes as there is only one key for the entire network, and it does not change with the addition of nodes. It has unacceptable drawback in robustness exists.

Pairwise keying model: When a new node is added to the network, the node must obtain a new key for communication. Adding new nodes to the network, may affect the flexibility requirement. This is a resource-intensive process that uses much more precious energy when compared with the simple preloading of a network-wide key as in the previous model. Some pairwise key distribution schemes, self-organization comes into question, because they tackle the scalability problem by reducing the number of shared keys, resulting in some nodes being unable to communicate with others and compromising the self-healing and self-organizing abilities of the network.

Group keying: scheme combines the features of both network and pairwise keying schemes. Within a group of nodes that form a cluster, communications are performed using a single, shared key similar to network keying. The communications between group's uses a different key between each pair of groups in a manner identical to the pairwise keying scheme. When one of the nodes is compromised, the compromise of the entire cluster that it belongs to, which is considerably more isolated than the entire network. Scalability is in the form of, increase keys with the number of groups, not with the size of the network. The problem with this scheme is that it is difficult to set up and also the formation of the groups is a very application dependent process. To efficiently distribute the keys, a keying scheme would require group formation information.

V. CLUSTERING SCHEMES

WSN [16] consists of hundreds or thousands of densely populated sensor nodes that sense the data and propagate through the network. They work collaboratively to process and sensed data. These sensor nodes send data streams to base stations either periodically or based on events and base station send the data to the destination node. In a network, sensors nodes may be densely populated wit, the area detected by the sensors are dividing into a number of small clusters. Each cluster has a coordinator or cluster head (CH), and a number of cluster nodes.

A. Base Station

The [18] [19] base station is a powerful node in the wireless sensor network and it can reach a wide range of communication area. The base station can be located at any place of the network, and it is not limited by electric power, memory space, or data-processing capacity. The base station serves as the gateway for external communication. If the base station has been invaded then the whole network will be taken over, so it is assumed that the base station is well protected and can always be trusted.

A sensor node is the core component of a WSN which can take on multiple roles in a network, such as sensing; data storage; routing; and data processing. It is assumed that sensor nodes are randomly distributed, and each node has a unique identity number. Sensor nodes are limited by electric power, memory space, computation capacity, and communication range. Clusters are the organizational unit for WSNs, dense nature of these networks requires the need for them to be broken down into clusters to simplify tasks such a communication.

B. Cluster Head Selection

Each [17] cluster has a coordinator or cluster head (CH). For CH selection any algorithm can be applied. In Cluster formation process, Firstly a cluster head is selected then with the collaboration of BS clusters are formed and finally routing is carried out. The cluster head selection phase starts and all the deployed nodes send their energy levels to the Base Station. Then on the basis of energy level, geographical area and least id cluster head are selected. Network deployment is considered as manual so the base station is well informed about the geographical locations of the nodes. Base Station will select the cluster heads and multicast this information. Cluster heads [18] are the organization leader of a cluster. A cluster [19] head is selected from the sensor nodes in the same cluster, so it has the same capacity and functions as the other nodes. They often are required to organize activities in the cluster. These tasks include but are not limited to data-aggregation and organization the communication schedule of a cluster

C. Cluster communication techniques

There are [17][18] two types communication techniques - a) Intra cluster communication b) Inter Cluster communication. In intra cluster communication, data transmission takes place between the nodes in a same cluster. In Inter Cluster communication, it takes place between the nodes of different cluster.

The clustering technique plays an important role not only for just organization of the network, but also on the network performance. There are several key limitations in WSNs, that clustering schemes must consider.

• Limited Energy: Unlike wired designs, wireless sensor nodes are ”off-grid”, meaning that they have limited energy storage and the efficient use of this energy will be vital in determining the range of suitable applications for these networks. The limited energy in sensor nodes must be considered as proper clustering can reduce the overall energy usage in a network.

• Network Lifetime: The energy limitation on nodes results in a limited network lifetime for nodes in a network. Proper clustering should attempt to reduce the energy usage, and hereby increase network lifetime.

• Limited Abilities: The small physical size and small amount of stored energy in a sensor node limits many of the abilities of nodes in terms of processing and communication abilities. A good clustering algorithm should make use of shared resources within an organizational structure, while taking into account the limitation on individual node abilities.

• Application Dependency: Often a given application will heavily rely on cluster organization. When designing a clustering algorithm, application robustness must be considered as a good clustering algorithm should be able to adapt to a variety of application requirements.

VI. MULTICASTING SCHEMES FOR SECURITY

1. Steiner –based Hierarchical secure multicast Routing protocol

2. Efficient CBMT with mobility aware MDSDV

A. Steiner-based Hierarchical Secure Multicast Routing Protocol

The details of secure multicast routing protocol [23] based on Steiner-based Hierarchical Multicast Routing Protocol, and we introduce the parameters of the proposed communication protocol

1) Nodes information gathering phase: In the secure multicast routing protocol, the source node should verify each node in order to prevent the malicious node to join in the network. We check the authentication of each node by pre-shared key. After the nodes randomly deployed inside, each node sends location information and HMAC to the source node

2) Steiner sub trees distribution phase: For the security reasons, the sensor node should unicast the node-state information table before broadcasting the topology of Steiner sub tree. And the secret keys of source node, Steiner sub tree and cluster need to be included in the message. So the source node executes .

3) Data delivery phase: In the phase of data delivering, the source node transmits multicast packets as the unicast data packet. After the data packet reaches the root node of the sub tree, CHs in the subtree forward the multicast packet in accordance with the order of Height Value. Simultaneously, if the CH detects that it is the destination, it first validate the time stamp T and the value of HMAC in the received message.

Secondly, each CH who is the destination of multicasting broadcasts the content of multicast packet Each MN in the cluster also checks T and value of HMAC. If the inequality holds and computing result is equal to HMAC in the received message, MNsaccept the content of multicast packet.

4) Steiner tree maintains phase: The main task of Steiner tree maintains is re-keying for each node in the network. In our proposed approach, we use the temporary session key to re-key the expired key

B. Efficient CBMT with mobility aware MDSDV

The proposed approach [24] is to achieve secure multicast communication for mobile adoc networks. The Approach uses Multicast version of DSDV routing protocol to maintain routing table periodically. It forms multicast tree among the group members. Each node can determine their present physical location. It quickly adapts to the topology changes. It is used to discover alternate route for failure of existing route. It also sends acknowledgement for each transmission in order to reduce the retransmission. Thus the approach of CBMT using MDSDV tends to have multicast connectivity between the nodes. The approach of Efficient CBMT with mobility aware MDSDV is described in five phases with specific notations.

Phase 1: Authentication: For each node, assign certificate key to verify its node identity. Each node has IP address, node address and certificate key. Certificate key and its IP address encrypt to form a public key. Thus, each node is authenticated based on broadcast request and reply.

Phase 2: Cluster Head Election: Initially the list of Local Controllers (LCs) contains only the source Group Controller GC. Then, GC collects all its 1 hop neighbours by MDSDV routing protocol. Elect LCs which are group members and which have child group members (the LC belongs to the unicast path between the source And the child group members). Verify for each one if it is a group member and if it has child group members then add the LC to the list of LCs. Thus, LCs are selected as cluster heads for its corresponding group members.

Phase 3: Cluster Formation: All the members reachable by this new LC will form a new cluster. If group members that exist and do not belong to the formed clusters then choose the nodes that have the maximum reachability to the others nodes in one hop from the remaining members. This reachability information is collected through the MDSDV routing protocol. Thus, nodes are selected as local controllers for the remaining group members and forms new cluster.

Phase 4: Secure Multicast Communication: The source encrypts multicast data with the TEK, and then sends it to all the members of the group following the multicast tree. The TEK distribution is achieved in parallel, according to the following steps. Initially, the entire group members receive from the source by unicast the session key KEKcsg-0 (key encryption key of the cluster sub-group 0), encrypted with their respective public keys. Each local controller should join this group. The local controllers decrypt this message, extract the TEK, re encrypt it with their respective clusters keys and send it to all their local members.

Phase 5: Node mobility: For frequent node mobility, a new member may join a group or an existing member may leave a group. To ensure secure multicast communication, both forward and backward secrecy has to be maintained. Forward Secrecy: When a node leaves the multicast group, it cannot decrypt the future data. It is known as leave operation. The leave operation is in two cases.

- When an ordinary node leaves, it gives less effect in multicast transmission.
    - When a local controller leaves, it leads to clusterization. It first sends the leave notification to the group controller and then all the members of the current LCs are merged with the other cluster based on the reachability information obtained by the MDSDV routing protocol

C. Comparison between two schemes

Security has the major impact on WSN in Multicast routing ,so two multicast scheme protocol is used to secure multicast data

Protocols	Steiner-based hierarchical secure multicast routing	Multicast version destination sequenced distance vector
Confidentiality	Data is not protected. it can be used by unauthorized	Data is protected .oly authorized users can use it
Fault tolerance	It does not tolerate the fault	It can tolerate the fault
Energy consumption	It consume more energy	less energy

VII. CONCLUSUON

In wireless sensor networks security is the major task to be provided in multicasting So we are using CBMT algorithm based on multicast version of DSDV(destination sequenced distance vector) routing protocol which provides secure communication in tolerating the fault less consumption and reduced packet drop ratio

REFERENCES:

[1]. Cheng-Lung Yang, WernhuarTarng, Kuen-Rong Hsieh and Mingteh Chen. "A Security Mechanism for Clustered Wireless Sensor Networks Based on Elliptic Curve Cryptography" IEEE 2010.

[2]. JaWonKo and Yoon-Hwa Choi "A Grid-Based Distributed Event Detection Scheme for Wireless Sensor Networks Sensors" 2011

[3]. XiaowangGuo ,Jianyong Zhu Research on "Security Issues in Wireless Sensor Networks" International Conference on Electronic & Mechanical Engineering and Information Technology IEEE 2011.

[4]. Ahmad Salehi S., M.A. Razzaque, ParisaNaraei, AliFarrokhtala "Security in Wireless Sensor Networks: Issues and ChallengesUniversity", Technologies Malaysia Skudai, MalaysiaIEEE 2013.

[5]. Hero ModaresRosliSallehAmirhosseinMoravejosharieh" Overview of Security Issues in Wireless Sensor Networks" Department of Computer system and technology University of Malaya Kuala Lumpur, Malaysia IEEE 2011.

[6]. Abhishek Jain, Kamal Kant M. R. Tripathy "Security Solutions for Wireless Sensor Networks" Department of Computer Science & Engineering ASET, Amity University Noida, India IEEE 2012.

[7]. Bin Tian, Yang Xin Shoushan LU0, Xi ouYang Dong , Li Zhe Gong , Yixian Yang "A Novel KeyMANAGEMENT METHOD FOR WIRELESS SENSOR NETWORKS Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, China IEEE 2010.

[8]. Zheng Yue-Feng, Han Jia-Yu, Chen Zhuo-Ran, Li Zheng A novel based-node level Security strategy in wireless sensor network Computer Department of Jilin Normal University BoDa College of Jilin Normal University Si Ping ,China IEEE 2012.

[9]. Adil Bashir, Ajaz Hussain Mir "An Energy Efficient and Dynamic Security Protocol for Wireless SensorNetwork Department of Electronics & Communication Engineering National Institute of Technology, Srinagar, Jammu & Kashmir, India IEEE 2013.

[10]. Thenmozhi, Dr.R.M. Soma sundaram Dean Towards an approach for improved security in Wireless Sensor Networks Department of Sciences SNS College of Engineering Coimbatore, India IEEE 2012.

[11]. SecurityYan-Xiao, Xi'an, Qian-Liang Research On Wireless Sensor Network Telecommunication Engineering Institute Air Force Engineering University Xi'an, Shaanxi, China IEEE 2010

[12]. T.Kavitha, S. JenifaSubhaPriya, Dr.D.Sridharan Design of Deterministic key pre distribution using number theory, Dept of

Electronics & Communication Engg College of Engineering, Guindy, Anna University Chennai, India IEEE 2011.

[13]. JaydipSenSecurity in Wireless Sensor Networks Department of Computer Science & Engineering, National Institute of Science & Technology, INDIA

[14]. David Martins and HervéGuyennetWireless Sensor Network Attacks and Security Mechanisms : A Short Survey Computer Science Department University of Franche-Comté, France IEEE 2010.

[15]. QusayIdreesSarhanaSecurity Attacks and Countermeasures for Wireless Sensor Networks: Survey Department of Computer Science, University of Duhsok, Iraq INPRESSCO 2013.

[16]. S. Jerusha, K.Kulothungan& A. KannanLocation Aware Cluster Based Routing In Wireless Sensor Networks International Journal of Computer & Communication Technology ISSN 2012.

[17]. Ketki Ram Bhakare R. K. Krishna SamikshaBhakareAn Energy-efficient Grid based Clustering Topology for a Wireless Sensor Network International Journal of Computer Applications 2012.

[18]. D. J. Dechene, A. El Jardali, M. Luccini, and A. Sauer A Survey of Clustering Algorithms for Wireless Sensor Networks.

[19]. Cheng-Lung Yang, WernhuarTarng, Kuen-Rong Hsieh and MingtehChenA Security Mechanism for Clustered Wireless Sensor Networks Based on Elliptic Curve Cryptography .IEEE 2010.

[20]. Wang Fangfang, Tao Jun, Shao BiruiAn Energy-Balanced Multicast Routing Algorithm in Wireless Sensor Networks IEEE. 2010

[21] Xin Li, ShuBoQiuResearch on Multicast Routing Protocol in Wireless Sensor Network. IEEE 2011

[22] ShahinMahdizadehAghdam,Mohammad KhansariOn the Better Performance of ADMR versus ODMRP 6'th International Symposium on Telecommunications (IST'2012)

[23] Rong Fan, Jian Chen, Jian-Qing FuLing-Di Ping A Steiner-Based Secure Multicast Routing Protocol for Wireless Sensor Network 2010 IEEE

[24] D.suganya Devi and Dr.Gpadmavathi “Efficient Cluster Based Multicast Communication” International journal Of engineering Science and technology 2010