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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayaShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A Trust Based Mechanism for Preventing Noncooperative Eavesdropping in WSN

Hemalatha.P[1], Mary Shyamala.L[2]

M.E, Dept of CSE, IFET College of Engineering, Villupuram, Tamil Nadu, India1

Associate Professor, Dept of CSE, IFET College Engineering, Villupuram, India[2]

ABSTRACT: The eavesdropping attack is a serious security threat to a wireless sensor network (WSN) since the eavesdropping attack is a prerequisite for other attacks. The traditional security solution based on cryptography and authentication is not sufficient for wireless sensor networks, which encounters new challenges from internal attackers, and trust is recognized as a novel approach to defend against such attacks. In this paper, we propose a trust-based LEACH (low energy adaptive clustering hierarchy) protocol for clustering to provide secure routing, while preserving the essential functionalities of the original protocol. Within the cluster, a measurable indirect trust of a CM (Cluster Member) is evaluated by its CH (Cluster Head). Thus each CM does not need to maintain the feedback from other CMs, which will reduce the communication overhead and eliminate the possibility of a Eaves Dropping attack by compromised CMs. A source and sink network is considered, and the intra cluster communication between the source and the sink is subject to non cooperative eavesdropping on each link. Without compromising any nodes an attacker can interrupt the network system. The proposed trust management detects the malicious behavior of the eavesdropped nodes. It is based on four trust components intimacy, honesty, energy, unselfishness of the nodes.

I. INTRODUCTION

A wireless sensor network (WSN) is usually composed of a large number of spatially distributed autonomous sensor nodes (SNs) to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. A SN deployed in the WSN has the capability to read the sensed information and transmit or forward information to base stations or a sink node through multi-hop routing. Traditionally trust is applied in various diverse domains such as e-commerce systems, ad-hoc networks, and peer-to-peer networks. In the clustered sensor networks, the cluster heads play a key role in relaying messages between the sensor nodes and the sink. While the cluster heads are involved in both intra-cluster and inter-cluster communication, the latter typically requires transmission over much longer distance than the former. It significantly improve time efficiency while reducing the effect of malicious nodes by maintaining canceling feedback between cluster members (CMs) or between CHs. The resource efficiency and dependability of a trust system are the most fundamental requirements for any wireless sensor network (WSN). Trust mechanism with the notion of trust in human society has been developed to defend against insider attacks. Since WSNs consist of hundreds or thousands of tiny sensor nodes, the trust mechanism is often implemented as a distributed system where each sensor can evaluate, update, and store the trustworthiness of other nodes based on the trust model. In general, trust mechanism works in the following three stages 1) node behavior monitoring, 2) trust measurement, and 3) insider attack detection. A lightweight trust decision-making scheme is proposed based on the nodes' identities (roles) in the clustered WSNs, which is suitable for such WSNs because it facilitates energy-saving in a sensor network considered and the communication between the source and the sink is subject to non cooperative eaves dropping on each link.

Within the cluster, a measurable indirect trust of a CM is evaluated by its CH. Thus each CM does not need to maintain the feedback from other CMs, which will reduce the communication overhead and eliminate the possibility of an Eaves Dropping attack by compromised CMs. The proposed scheme is optimal and agreeable, i.e., it achieves the secure

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayaShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

communication within a cluster. By Establishing trust in a clustered environment provides numerous advantages, such as enabling a CH to detect faulty or malicious nodes within a cluster.

II. MOTIVATION

The advances of today's communication networks, both wired and wireless, have dramatically improved their accessibility and affordability. As such, people have become increasingly dependent on their ability to stay connected, both in their personal and professional lives. Traditional research work in wireless sensor networks is mostly based on the assumption of a trusted environment which may not be realistic for every application. Traditional trust management schemes that have been developed for wired and wireless ad-hoc networks are not suitable for wireless sensor networks because of higher consumption of resources such as memory and power resources such as memory and power.

1)Maintaining the integrity and security of the information flowing over the ever pervasive networks is providing the critical importance for both privacy concerns and business or national security reasons. Universal trust system designed for clustered WSNs for the simultaneous achievement of resource efficiency and dependability remains lacking

2)Moreover, WSNs are easy to be attacked by the way that traditional networks have never met, such as node capture, Eaves Dropping, sniffer, deny of service, worm hole and sybil attack etc. Thus, we need a mechanism that can effectively identify the captured nodes and take appropriate measures to reduce system loss.

3)The resource efficiency and dependability of a trust system are the most fundamental requirements for WSNs. However, existing trust systems developed for clustered WSNs are incapable of satisfying these requirements because of their high overhead and low dependability. Also, implementing complex trust evaluation algorithms at each CM or CH is not practical.

4)In existing trust mechanisms, trust management systems collect remote feedback and then the feedbacks from all the nodes are aggregated to obtain the global reputation which can be used to evaluate the global trust degree(GTD) of this node. Due to the broadcast nature of the WSN environment, it contains a large number of undependable (or malicious) nodes. Feedback from these undependable nodes may result in the incorrect evaluation of feedback. So a trust system should be highly dependable in terms of providing service in an open WSN environment.

III. RELATED WORKS

1. *T Morkel , JHP Eloff* [1] proposed Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. Very expensive to encrypt and decrypt power. But the algorithm takes a lot of processing, energy and computer power as well. Algorithm designed for 1970s hardware implementation. It performs sluggishly in software implementations 3DES is 3 times slower due to 3 rounds64 bit block size needs to be increased to speed things up.
2. ***Lei Huang*** *[2]* proposed Watchdog is a monitoring mechanism introduced to identify the misbehaving nodes in the network .In this approach each sensor node has its own watchdog that monitors and records its one hop neighbors' behavior such as packet transmission**.** When sending node A sends a packet to its next node B, the watchdog in A verifies whether B forwards the packet to the next node or not by using its overhearing ability within its transceiver range as shown in Figure 1.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayaShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

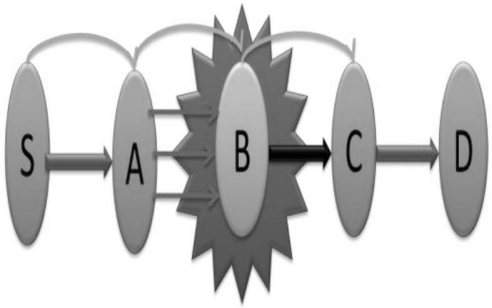

Figure 1: Watch Dog Mechanism

Evaluates its next-hop's behavior and propagates the evaluation result to other nodes by broadcasting, which is neither energy efficient nor attack resilient. Since the mechanism has some disadvantages such as Ambiguous collision, Receiver collision, Limited transmission power, False misbehavior, Partial dropping.

3. Jin Xu and Biao Chen[3] proposed ford fulkerson algoritm+shannon key encryption

The idea behind the algorithm is simple. As long as there is a path from the source (start node) to the sink (end node), with available capacity on all edges in the path, we send flow along one of these paths. Then we find another path, and so on. A path with available capacity is called an augmenting path as shown in figure 2

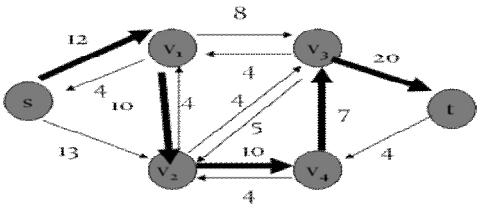

Figure 2:Example for augmenting path (bold edges)

a) No secret key is available *a priori to the source and the sink* nodes. Nonetheless, Shannon's cipher system is inherently useful for such a network setting when there exists route redundancy between the source and the sink nodes.

b) The transmission in each link of the network is subject to non cooperative eavesdropping. Alternatively, there is single adversary, but the link that the adversary chooses to eavesdrop is unknown to the communicating parties.

c) The main contribution of this mechanism is to obtain an achievable rate equivocation region that characterizes **the tradeoff between the communication rates and confidentiality.**

d) It combines the classical Ford–Fulkerson algorithm for max-flow min-cut network flow and the one-time pad scheme to achieve the desired rate equivocation tradeoff.

e) Existing result is consistent with that of secure network coding when it imposes the perfect secrecy constraint. More importantly, the constructive proof to the achievability constitutes a secure communication scheme that combines the Ford–Fulkerson algorithm and the one-time pad scheme which is both intuitive and easy to implement **but yet vulnerable to attacks.**

The Algorithm is as follows

FORD-FULKERSON-METHOD(G,s,t)
initialize flow *f* to *0*
while there exists an *augmenting* path *p*

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayaShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

do *augment* flow *f* along *p*
return *f*

4. **Bao *et al.*** [4] proposed HTMP, a hierarchical dynamic trust management protocol for cluster-based WSNs that considers two aspects of trustworthiness: social trust and QoS (quality-of- service) trust. The authors developed a probability model utilizing stochastic Petri net techniques to analyze protocol performance and then validated subjective trust against the objective trust obtained based on ground truth node status. However, implementing such a complex trust evaluation scheme at each CM of the cluster is unrealistic.
5. **Crosby *et al***. [5] proposed TCHEM, a trust-based cluster head election mechanism. Its framework is design in the con- text of a cluster-based network model with nodes that have unique local IDs. This approach can decrease the likelihood of malicious or compromised nodes from becoming CHs. The mechanism does not encourage sharing of trust information among sensor nodes. Thus, this approach reduces the effect of bad mouthing attacks. However, TCHEM does not cover trust in detail, because of which numerous key issues of trust management are not introduced.
6. **Boukerche *et al***[6] proposed ATRM, an agent-based trust and reputation management scheme. ATRM introduces a trust and reputation local management strategy with the aid of the mobile agents running on each node. The benefit of a local management scheme for trust and reputation is that central- ized repositories are not required, and the nodes themselves capable of providing their own reputation information whenever requested. Therefore, reputation computation and propagation is performed without network-wide flooding and with no acquisition-latency. However, ATRM assumes that mobile agents are resilient against malicious nodes that try to steal or modify in- formation that such agents carry. In numerous applications, this assumption may be unrealistic.

IV. PROPOSED SYSTEM

Recent wide spread uses of sensor networks have evoked the need of proper lightweight trust management schemes. The main contributions of the project are

1. Using clustering algorithm LEACH Low-Energy Adaptive Clustering Hierarchy, the sensor nodes are grouped into clusters, and within each cluster, a node with strong computing power is elected as a cluster head (CH). Each sensor elects itself to be Cluster Head at the beginning of a round. Nodes that have not already been cluster heads recently, may become cluster heads CHs together form a higher-level backbone network. After several recursive iterations, a clustering algorithm constructs a multilevel WSN structure.
2. Within the cluster, a measurable indirect trust of a Cluster Member CM is evaluated by its CH. The transmission in the intracluster of the sensor network is subject to non co-operative eavesdropping. In which, there is a single adversary, but the link that the adversary chooses to eavesdrop is unknown to the communicating parties. The eaves dropping nodes are not synchronize with one another and no collisions are occurring among them.

3.All CMs communicate via a shared bidirectional wireless channel and operate in the promiscuous mode, that is, if a source node sends message to CH via cluster members , then CMs can hear whether node forwarded such message to CH and to the destination. If a node overhear the retransmission of the packet within a threshold time from its neighboring node it is considered as a trusted node or if the overheard packet is found to be illegally fabricated and it is considered as eavesdropped node.

4.The proposed mechanism as shown in figure 3 identifies the broken-down nodes and captured nodes by calculating the trust degree of sensor nodes in the intracluster communication as shown in figure 4. Respective node's trust value known by all nodes inside the cluster (intracluster), so malicious nodes cannot easily attack

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayaShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

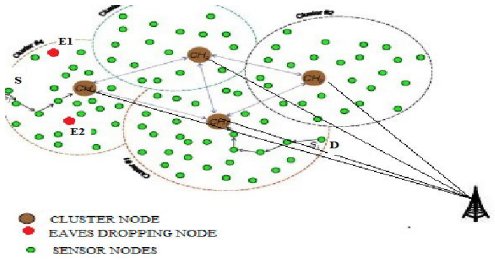

Figure 3:System Architecture

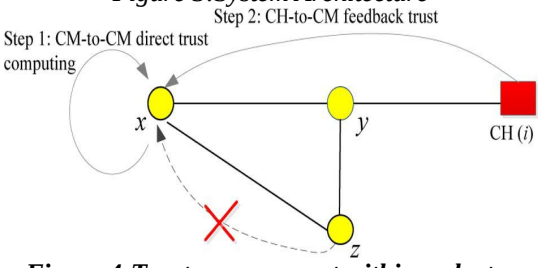

Figure 4:Trust management within a cluster

V. CLUSTERING ALGORITHMS

LEACH stands for Low-Energy Adaptive Clustering Hierarchy. Each sensor elects itself to be cluster head at the beginning of a round. Nodes that have not already been cluster heads recently, may become cluster heads .Probability of becoming a cluster head is set as a function of nodes' energy level relative to the aggregate energy remaining in the network.LEACH consists of Two phases

1.set up phase
2.steady state phase

1. Cluster Formation (SETUP PHASE)

a) Each cluster head node broadcasts an advertisement message (ADV) using CSMA MAC Protocol
b) The message consists of the nodes' ID and a header that distinguishes it as an ADV message
c) Each non-cluster head node determines its cluster/cluster head that requires minimum communication energy
d) Largest signal strength, minimum transmit energy for communication
e) Each node transmits a join-request message (REQ) using CSMA MAC Protocol
f) The message consists of node's ID and cluster head ID
g) Each cluster head node sets up a TDMA schedule and transmits it
h) This ensures that there is no collision in data messages, radio components can be turned off at all times except during transmit time.

2. STEADY STATE PHASE

a) Nodes send data during their allocated time slot
b) Once the cluster head receives all data it performs data aggregation
c) Resultant data is sent from cluster head to BS (a high energy transmission)as in figure 12
d) Uses transmitter based code assignment to reduce inter-cluster interference
e) Cluster head senses the channel before transmission.

The LEACH algorithm is depicted as in figure 5

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayaShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

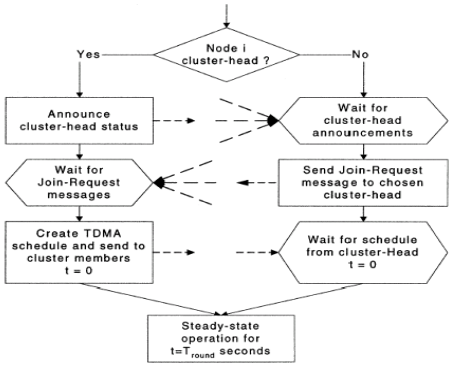

Figure 5:Network flow of LEACH algorithm

VI. IMPLEMENTATION AND RESULTS

The software developed is to detect the attack in the wireless sensor networks. the various modules have been implemented using Network Simulator Version 2 (ns2) in the network layer, where the mobile nodes have been established in the WSN topology. The basic modules to be implemented are Network Creation, Cluster Formation, Injecting Non Cooperative Eavesdropping, Preventing Non Cooperative Eavesdropping.

A. Network Creation

In this module a wireless sensor network topology is created with specific number of nodes. One sensor node sends packets to the destination node at a specific time. The network creation involves the following steps.

a) Create node position
b) Create a duplex link between the nodes
c) Create a UDP agent and attach it to node
d) Create a Null agent (a traffic sink) and attach it to node
e) Create agent and attach it to corresponding nodes
f) Add the Traffic
g) Add application for the routing traffic

B .Cluster Formation

In this module wireless sensor network topology with specific nodes are divided into clusters by using LEACH routing protocol. LEACH stands for Low-Energy Adaptive Clustering Hierarchy.

a) Each sensor elects itself to be cluster head at the beginning of a round. Nodes that have not already been cluster heads recently, may become cluster heads.
b) The LEACH network has two phases: the set-up phase and the steady-state
   i.The Set-Up Phase-Where cluster-heads are chosen
   ii.The Steady-State-The cluster-head is maintained and data is transmitted between nodes
c) After forming clusters the source node sends the packets to the destination node within the cluster.
d) A source node sends packets to the destination node through multi hop networking , the packets are transmitting via routing nodes through which a cluster member (CM) can send data to the CH and cluster head retransmitting to the desired CM

C.Injecting Non Cooperative Eavesdropping

In this module two or more malicious nodes are injected among nodes into a cluster that are not transmitting the packets with a specific period of time.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayaShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

a) With this threat, links in the network are subject to eavesdropping, but no collusion(Secret or illegal cooperation) is allowed among eavesdroppers on different links.
b) A single adversary who may eavesdrop on any single link of his/her choice and the link that is subject to eavesdropping is unknown to the communicating parties.
c) An end to end delay is encountered while sending the data to the destination.
d) The malicious nodes are easily identified by the trust values possessed by the Cluster Heads(CH)

D.Preventing Non Cooperative Eavesdropping

In this module the source sends the packets to the destination inside the cluster by maintaining the individual trust values

a) Every node will be assigned with individual trust value 0s and 1s.
b) Assuming the time limit for sending packets is set 1.0sec .If there is no End to End delay then the node is a trusted node posses trust value 1
c) If the node has transmitting delay it is a eavesdropping node posses trust value 0.,means that no packet are let to transmit in that path
d) Respective node's trust value known by all node inside the cluster (intracluster),so malicious nodes cannot easily attack.

VIII. CONCLUSION

Research on trust management scheme for wireless sensor network is at very infancy state and current sensor network security solutions are based on assumption of trusted environment .Therefore In this work, we proposed Trust Management scheme for clustered WSNs. Given the cancellation of feedback between nodes, it can greatly improve system efficiency while reducing the effect of malicious nodes. By using dependability-enhanced trust evaluating approach for cooperation's between CHs, the proposed system can effectively detect and prevent malicious, selfish, and faulty CHs. Wireless Sensor Networks are vulnerable to a wide set of routing-related attacks. To defend against these attacks, the nodes monitor the behavior of their neighbours and calculate their trustworthiness which is then used to make trust-aware decisions. By adopting the principle of the highest trust route, we can low down the calculation complexity and risk of the model to some extent

1X. REFERNCES

[1] T Morkel , JHP Eloff, "Encryption Techniques for wireless microsensor net- works," IEEE Trans. Wireless Commun., vol. 1, no. 4, pp. 660–670, Oct. 2002.

[2] Lei Huang, "Extended Watchdog Mechanism For WSN" Comput. Commun., vol. 32, no. 4, pp. 662–667, Apr. 2009.

[3] Jin Xu and Biao Chen," Secure Coding Over Networks AgainstNoncooperative Eavesdropping" IEEE Transactions On Information Theory, VOL. 59, NO. 7, JULY 2013

[4] F. Bao, I. Chen, M. Chang, and J. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," IEEE Trans. Netw. Service Manag., vol. 9, no. 2, pp. 169–183, Jun. 2012.

[5] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," in Proc. Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems, 2006, pp. 10–22.

[6] A. Boukerche, X. Li, and K. EL-Khatib, "Trust-based security for wire- less ad hoc and sensor networks," Computer Commun., vol. 30, pp.2413–2427, Sep. 2007.

[7] D. Kumar, T. C. Aseri, and R. B. Patel, "EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks," Comput. Commun., vol. 32, no. 4, pp. 662–667, Apr. 2009.

[8] Y. Jin, S. Vural, K. Moessner, and R. Tafazolli, "An energy-efficient clustering solution for wireless sensor networks," IEEE Trans. Wireless Commun., vol. 10, no. 11, pp. 3973–3983, Nov. 2011.

[9] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, dis- tributed clustering approach for Ad-Hoc sensor networks," IEEE Trans. Mobile Comput., vol. 3, no. 4, pp. 366–379, Oct. 2004.

[10] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Trans. Sensor Netw., vol. 4, no. 3, pp. 1–37, May 2008.