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, Issue 2, February 2014

Energy-efficient and Secured Data Gathering in Wireless Multimedia Sensor Networks

T.N.Prabhu[1], C.Ranjeeth Kumar [2], B.Mohankumar[3]

Assistant Professor, Information Technology, Sri Ramakrishna Engineering College, Coimbatore, India[1]

Assistant Professor, Information Technology, Sri Ramakrishna Engineering College, Coimbatore, India [2]

Lecturer, Information Technology, Sri Ramakrishna Engineering College, Coimbatore, India [3]

ABSTRACT: A Wireless Multimedia Sensor Network (WMSN) is often partitioned into a set of spatial clusters to save energy for data collection. Each cluster includes sensor nodes with similar sensing data, and only a few sensor nodes (samplers) report their sensing data to a base node. Then the base node may predict the missed data of non-samplers using the spatial correlation between sensor nodes. The problem is that the WMSN is vulnerable to internal security threat such as node compromise. If the samplers are compromised and report incorrect data intentionally, then the WMSN should be contaminated rapidly due to the process of missed data prediction at the base node. In this paper, we propose Energy-Efficient Secure Routing algorithm to detect compromised nodes for secure data collection in the WMSN. Experiment results indicate that the proposed algorithm can detect compromised nodes with a high accuracy and an energy-efficient manner.

KEYWORDS: Wireless Multimedia Sensor Network, Security, Data collection, Node compromise, Trust Value evaluation

I. INTRODUCTION

Wireless Multimedia Sensor Networks (WMSNs) have drawn a lot of attention recently due to their broad applications in both military and civilian operations. A WMSN usually consists of a large number of ultra-small, low-cost devices that have limited energy resources, computation, memory, and communication capacities and for the applications such as battle field reconnaissance and homeland security monitoring. WMSNs are often deployed in a vast terrain to detect events of interest and deliver data reports over multi-hop wireless paths to the sink. Data security is essential for these mission critical applications to work in unattended and even hostile environments [9]. One of the most severe security threats in WMSNs is security compromise of sensor nodes due to their lack of tamper resistance. In WMSNs, the attacker could compromise multiple nodes to obtain their carried keying materials and control them, and thus is able to intercept data transmitted through these nodes thereafter. As the number of compromised nodes grows, communication links between uncompromised nodes might also be compromised through malicious crypto analysis. Hence, this type of attacks could lead to severe data confidentiality compromise in WMSNs. Furthermore, the attacker may use compromised nodes to inject bogus data traffic into WMSNs. In this attack, compromised nodes pretend to have detected an event of interest within their vicinity, or simply fabricate an bogus event report claiming a non-existing event at an arbitrary location. Such insider attacks can severely damage network function and result in the failure of mission-critical applications. They may also induce network congestion and wireless contention, and waste the scarce network resources such as energy and bandwidth, hence, severely affecting both data authenticity and availability. Lastly, the attacker could use compromised nodes to launch selective forwarding attacks, in which compromised nodes selectively drop the going through data traffic and thus to severely jeopardize data availability.

The existence of the aforementioned attacks together with the inherent constraints of sensor nodes, make it rather challenging to provide satisfactory data security in WMSNs with respect to all its three aspects, i.e., confidentiality, authenticity and availability. Node compromise is a major type of internal attacks. Compromised sensor nodes release all the security information to the adversary. Then, the adversary can easily launch internal attacks with data

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, Issue 2, February 2014

alteration, message negligence, selective forwarding, and jamming. Note that the node compromise is especially problematic for

periodic data collection, where only the samplers may report data to the base node. If the samplers are compromised and report incorrect data intentionally, then the WSN should be contaminated rapidly due to the process of missing data prediction at the base node. This means that detecting and defending against node compromise are inevitable tasks to guarantee the correctness of data collection at the WMSN.

To provide secured sensory data delivery, some security mechanisms have been developed for based on traditional key establishment, authentication, access control, etc. Unfortunately, these security mechanisms cannot provide

satisfactory solutions to the internal attack, which can easily acquire the valid cryptographic keys and intercept any packet transmitted through the compromised node. Besides the network security, another critical issue is minimizing overall energy consumption of WMSNs. In fact, energy efficiency is always an important requirement in the applications of sensor networks. Although WMSNs are developed from traditional sensor networks, energy limitation is more severe due to the high quantities of sensory data including multimedia content. Moreover, the image and video sensor nodes are deployed in sparseness for their strong directives and far-field of view, which increase the energy consumption dramatically. Taking above issues into consideration, we propose a novel routing scheme called energy-efficient secure routing (ESR), which combines security and energy as selection criteria to build routes.

The main contributions of this paper are three folds.

1. We study the random attack behaviours of compromised sensor nodes in WMSN, which may change dynamically and cannot be reflected without priori knowledge. It provides the necessary condition for compromised nodes detecting;

2. We propose a novel trust evaluation model to detect compromised sensor nodes. Using this evaluation model, sensor nodes can effectively identify compromised nodes from their neighbours without the priori knowledge;

3. We propose the ESR scheme to build routes from source nodes to sink node. With the proposed ESR routing, the compromised sensor nodes can be early detected and bypassed during data collection. In addition, the process of routing establishment and maintenance is energy-efficient.

II. RELATED WORK

This paper is closely related to security mechanisms in sensor networks, which can be divided into three kinds of research: Sensory reading fault identification, unusual activity detection and node misbehaviour detection. In the following discussion, we briefly review the existing proposals.

2.1. Sensory reading fault identification

The detection and reporting of the occurrence of an interesting event is one of the important tasks of sensor networks. Due to limitations in available resources, such as power, memory and computing capability, sensor nodes deployed in a harsh environment, operating in an unattended mode, are prone to failure [1]. Faulty nodes might issue an alarm even though they are not in an event region. They degrade the network reliability, unless some provisions are made to tolerate them. Each sensor node receives the sensor readings of neighboring nodes and makes a decision on an event locally in a distributed manner to identify the faults.

2.2. Unusual activity detection

Due to their broadcast nature, wireless networks are more susceptible to attacks. Adversaries can exploit vulnerabilities in the physical and the medium access control layers, and heavily disrupt the communication between the network nodes [2]. Intrusion detection involves the automated identification of unusual activity by collecting audit data, and comparing it with reference data. A primary assumption of intrusion detection is that a network's normal behaviour is distinct from abnormal or intrusive behaviour.

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, Issue 2, February 2014

2.3. Node misbehaviour detection

Our approach to misbehaviour detection in WSN relies on the ability of a given wireless device (node) to efficiently analyze its own states and events as well as all observable events and states in its physical neighbourhood [4]. A neighboring node is said to be in the physical neighborhood of a node, if this given node is able to overhear the traffic of the neighboring node. All states and events are evaluated and averaged over a sliding time window. Each node in the network runs an instance of the learning algorithm. This implies that each node is able to detect whether one of his neighbors is likely to misbehave. Our approach currently does not include any exchange of detection information, there is no collective evaluation of misbehaviour and it does not support any actions that would be able to suppress or

eliminate the consequences of misbehaviour on a sensor network. Operation in promiscuous mode is rather energy inefficient since the node has to stay on all the time. There have been several approaches aimed at energy preservation at nodes. One of the approaches suggests, each node should publish its listen-sleep schedule.

III.BACKGROUND MODELS AND GOALS

3.1. System Model

We assume that the sensors are deployed such that their locations are distributed uniformly at random in a desired area. In our model, the network is relatively dense (e.g., more than ten one-hop neighbors per sensor) so there are multiple neighbors which a sensor can overhear. Our analysis also assumes a radio model that can be represented by unit disks and that links are asymmetric; so if A can hear B, then B cannot hear A. The plan is to implement the protocol do determine the effects of a more realistic physical layer. We assume that the sensors can communicate on multiple, non-interfering channels, but can only listen to or transmit on a single channel at any given time.

3.2. Threat Model

As a general wireless sensor network environment, sensor nodes in the network are deployed in open areas, so they are confronting the added risk of physical attacks. Because sensor networks have many opportunities to interact closely with anonymous adversaries, deceitful data from them can be easily accepted as legal data in the networks [3]. In addition, because each sensor node is vulnerable to a node capture attack, some private keys used for secure communication in the networks can be snatched by active attackers.

3.3. Goal

We focus on making resilient wireless sensor networks which work normally even though some sensor nodes might be compromised. Without any trust evaluation mechanisms, we cannot guarantee the sensor networks to work appropriately even if the networks adopt cryptographic key management approaches.
For the purpose of the resilience of sensor networks, we direct our approaches to evaluate trustworthiness of sensor nodes, and filter out inconsistent and deceitful data from the malicious or compromised nodes.

IV. TRUST EVALUATION MODEL

Trust evaluation model is essential to distinguish forged data of illegal nodes from innocent data of legal nodes in sensor networks. In this paper, to make resilient wireless sensor networks, we propose a trust evaluation model which can identify trustworthiness of sensor nodes in order to filter out malicious nodes deceitful data. It is done by calculating the initial trust value and the comprehensive trust value. Trust Evaluation Model is shown in Fig 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, Issue 2, February 2014

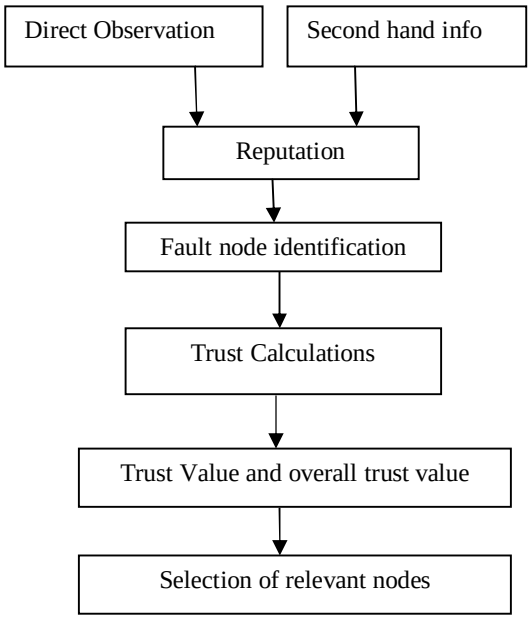

Fig: 1 Trust computational model for WMSN

4.1 Trust Metrics

To evaluate the trustworthiness of a sensor node, multiple aspects of its behaviour can be monitored. Each of them aims at detecting a specific type of attack. For example, each time node s1 selects node s3 for forwarding its packet it enters the promiscuous mode in order to check whether node s3 successfully forwarded it. After a number of cooperations, comparing the successfully forwarded packets to the number of packet s1 sent to s3, the source node (node s1) can assess the sincere execution of the routing protocol while a systematic failure reveals a selfish and/or malicious node acting as a black hole. Similarly, measuring the packets correctly forwarded without being modified, Nodes issuing modification attacks can be detected. Both the direct and indirect measurements may address more than one node behaviours (e.g. forwarding and availability). Examining the above behaviour list, it is obvious that the required processing to decide whether a data message has been actually forwarded is less than the processing required to check the message precision and significantly less than the processing required to decide on the consistency of the reported data.

4.2 Trust Evaluation

In this step, sensor nodes evaluate trustworthiness of other nodes. However, each sensor node does not compute all the other nodes' trust values in the networks, but computes only its neighbor nodes' trust values accumulatively. Each sensor node has a trust evaluation matnx which stores the trust evaluation factors for its neighbor nodes. The node 0 has k trust evaluation matrices for its k neighbor nodes [5]. The trust evaluation matrix consists of several trust evaluation factors as follows.

a) Sensing communication

This factor contains communication ratio information. When a node detects a certain event, if its neighbour nodes also detect the same event and broadcast the sensing results, communication ratio values for those neighbor nodes go up. If they do not communicate, communication ratio values for those nodes **go** down. This factor represents the level

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, Issue 2, February 2014

of selfishness and normality of a node. If a node does not participate in communication in the networks continuously for its battery saving or some other Roubles, its trust value will be degraded.

b) Sensing result

This factor represents sensing result information for detected events. This factor consists of sensing data and sensing time for the events. The information of this factor is used to check a consistency of each sensor node and to detect illegal or compromised nodes in the networks.

c) Consistency

This factor represents a level of consistency of a node. Based on this factor, we can identify malicious or compromised nodes, and filter out their data in the networks.

d) Battery

This factor represents remained lifetime of a sensor node. As we compute trust values in consideration of this factor, we can reduce additional processes which would be necessary to handle some power managing policies. In addition, some nodes which have high trust values are likely to process more jobs than the other nodes which have low trust values. In that case, the higher trust value a node has, the earlier the node meets its end. According to the adoption of this battery factor, we can prevent such a biased battery exhaustion.

e) Trust value

This factor represents **a** total trustworthiness of a node, which is evaluated based on the other trust evaluation factors. Trust value **of** a node is dynamic because the values of each trust evaluation factor change with the lapse of time.

4.3. Overall Trust or Comprehensive Trust Value

Trust depends on a subject's (evaluating node) observation on the object (evaluated node) and third party recommendations. The WMSNs' features need a trust evaluation mechanism [7] without central nodes, where neighbor nodes monitor each other. The subject obtains the trust value of objects according to both direct and indirect trust values. The node *i* is subject, which not only makes direct assessment of object *j*, but also makes indirect evaluation of the object j through nodes k_1, k_2, k_3.Generally, the evaluated object has many neighbor nodes, and every neighbor has the direct trust value and indirect trust value of the evaluated object. We use the membership function of nodes' trust classification to calculate the basic confidence level of trust evidence to the 'Distrust', 'Uncertain', 'Trust' propositions of nodes. Then the integrated trust value of the object is acquired by composing the direct and indirect trust value.

V. SECURED ROUTING AND ENERGY EFFICIENT METHOD

It has been proved that the tasks performed by the sensor nodes that are related with communications (transmitting and receiving data); spend much more energy than those related with data processing and memory management[8]. Since one of the main concerns in WMSN is to maximise the lifetime of the network, which means saving as much energy as possible, it would be preferable that the routing algorithm could perform as much processing as possible in the network nodes, than transmitting all data through the ants to the sink-node to be processed there[11]. In fact, in huge sensor networks where the number of nodes can easily reach more than 1000 units, the memory of the sensors would be so big that it would be unfeasible to send the packets through the network. A memory must be created at each node that keeps record of each sensor data that was received and sent. Each memory record saves the previous node, the forward node and a trust value. Whenever a forward data is received, the node looks into trustable or not. If no record is found, the node saves the required information and forwards the data to the next node. If a record contains that the sensor node is trustable, then it forwards the data through that node. When a node receives a trust value of the neighbour node below the threshold value it searches for other node where both the trust value and energy is maintained.

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, Issue 2, February 2014

VI. PERFORMANCE EVALUATION

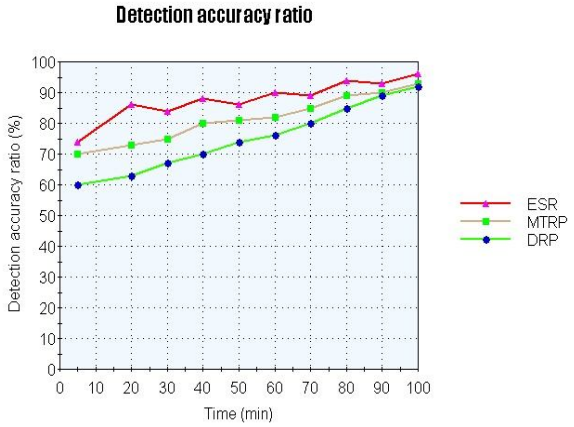

Fig:2 Detection Accuracy Ratio

VII. CONCLUSIONS

In this paper, an energy efficient secure routing protocol is proposed to deliver the message to the sink correctly without any alterations. It is a routing protocol with security mechanism to defense the attacks. Detection of compromised node is done by forwarding messages between various sensor nodes. We also propose energy efficient secure routing protocol to deliver the message to the sink correctly without any alterations. It is a routing protocol with security mechanism to defence the attacks. The implementation of our routing protocol is feasible. The performance of our routing protocol is also shown to be energy efficient. We follow several testing standard and assume some reasonable routing topology to calculate the performance.

REFERENCES

[1] Sung-Jib Yim and Yoon- Hwa Choi , An Adaptive Fault-Tolerant Event Detection Scheme for Wireless Sensor Networks, March 2010.
[2] Alexandros G. Fragkiadakis, Vasilios A.Siris, and Nikolaos Petroulakis , Anomaly-Based Intrusion Detection Algorithms for Wireless Networks, Foundation for Research and Technology – Hellas,2010.
[3] Junbeom Hurt, Younho Leet, Hyunsoo Yoont , Daeseon Choit and Seunghun ,Trust Evaluation Model for Wireless Sensor Networks Division of Computer Science 2005.
[4] Matthias Becker Martin Drozda Sven Schaust Sebastian Bohlmann Helena Szczerbicka , On Classification Approaches for Misbehavior Detection in Wireless Sensor Networks, journal of computers, vol. 4, no. 5, May 2009.
[5] Tiago Camilo, Carlos Carreto, Jorge Sá Silva, Fernando Boavida ,An Energy-Efficient Ant-Based Routing Algorithm for Wireless Sensor Networks, Laboratory of Communications and Telematics 2002.
[6] Mohammad Hossein Anisi, Abdul Hanan Abdullah, Shukor Abd Razak, Energy-Efficient Data Collection in Wireless Sensor Networks, Department of Computer Systems and Communications 2011, 3, 329-333.
[7] Renjian Feng, Xiaofeng Xu, Xiang Zhou, and Jiangwen Wan, A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors IEEE Symposium on Security and Privacy; Oakland, CA, USA 2011 January 25.
[8] Ganesh.S and Dr.R.Amutha (2012) 'Efficient and Secure routing protocol for wireless sensor network using mine detection" ICCM 2012,International conference on computing technology and information management,Vol3.,March 2012.
[9] Akyildiz I.F., Su W., Sankarasubramaniam Y., Cyirci E. Wireless sensor networks: a survey. Comput. Net. 2002.

BIOGRAPHY

Mr. T.N.Prabhu received his bachelor degree in information technology from Anna University Chennai, India and his master degree in information technology from the same university. He has published many papers in international journals and conferences. He is currently working as assistant professor, department of information technology, Sri Ramakrishna Engineering College, Coimbatore, India. His research areas are wireless multimedia sensor networks, image processing, cloud computing, service

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, Issue 2, February 2014

oriented architecture and semantic web.

Mr. C.Ranjeethkumar received B.Tech. Degree in Information Technology from Dr.Mahalingam college of Engineeringand Technology, Pollachi and received my M.E. Degree in Computer Science and Engineering from Sri Krishna College of Engineering and Technology, Coimbatore. Presently working as Assistant Professor in the Department of Information Technology at Sri Ramakrishna Engineering College, Coimbatore. His research areas are Wireless Networks, Image Processing.

Mr. B.Mohankumar received B.Tech. Degree in Information Technology from Sri Ramakrishna Engineering College, Coimbatore and pursuing M.Tech. Degree in Information Technology from Anna University, Regional Centre Coimbatore. Presently working as Lecturer in the Department of Information Technology at Sri Ramakrishna Engineering College, Coimbatore. Area of interest is Networks, Data Mining, Cloud Computing and Data Security.