International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume3, Issue 4 (April '2017)

TRUST MANAGEMENT IN UNATTENDED WIRELESS SENSOR NETWORKS

V.R.Ramesh,
M.Phil Scholar,
Department of Computer Science and Applications,
Mahendra Arts and Science College,
Kallipatti,Namakkal.

N.Suresh,
Assistant Professor,
Department of Computer Science and Applications,
Mahendra Arts and Science College,
Kallipatti,Namakkal.

Abstract: An Unattended Wireless Sensor Network is a type of sensor network where a trusted sink visits each node periodically to collect the data. Due to offline nature of this network, every node has to secure the sensed data until next visit of the sink i.e. until data is being sent to the sink. The goal of an attacker is to prevent targeted data from ever reaching the sink or to send corrupted data to the sink. So, in a UWSN data confidentiality and data authenticity are required. Besides have to take care of survivability of sensed data. In this paper we have presented a scheme that provides authenticity, confidentiality and survivability of sensed data in efficient manner.

Keywords: Unattended Wireless Sensor Network, Trust Management System Attacks

I.INTRODUCTION

Unattended Wireless Sensor Networks (UWSN) is a hybrid type of WSN where data sensed by the sensors is not collected continuously by the sink. Data has to be secured by every node until the next visit of the mobile sink. This inability to communicate with sink might be for reasons such as: limited transmission ranges, power constraints or signal propagation problems. The concept of UWSNs with a mobile sink looks realistic if we consider the environments where the sensing field is too far from the base station and sending data through intermediate nodes may result in weakening the security (e.g., intermediate nodes may modify the data) or increase the energy consumption of the nodes close to the base station. In normal multi-hop Wireless Sensor Networks, power of the nodes placed near the sink will be depleted earlier than the other nodes. This is because all the nodes have to transmit the data to the sink through the nodes placed near the sink. An UWSN can be used to save the battery of these nodes and as a result increase the lifetime of the network Unattended environments as mentioned in [1] include sensor networks for monitoring sound and vibration produced by troop movement, airborne sensor networks for tracking enemy aircrafts, LANdroids [2] which retain information until soldiers move close to the network, sensor networks for monitoring nuclear emissions, national parks for firearm discharge and illicit cultivation, etc.

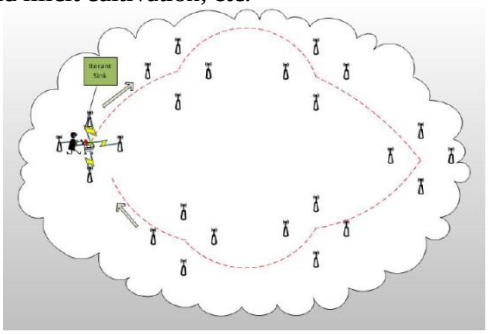

Figure 1: Unattended Wireless Sensor Network with Mobile Sink collecting the data

Applications of UWSNs

Applications of UWSNs as mentioned in [1] include

1. Network of nuclear emission sensors deployed to monitor any potential nuclear activity.
2. Underground sensor network aimed at monitoring the troop movements.
3. Airborne sensor network tracking fluctuations in air turbulence and pressure to detect enemy aircrafts.
4. Monitoring system to detect poaching in a national park.
5. Submarine sensor network to track the movements of animals.
6. Monitoring underground or underwater oil pipelines to detect the leakage of oil.
7. A WSN mounted on a tree to monitor firearm discharge or illegal cutting of the trees.
8. A sensor network deployed in the international border to monitor illegal crossings.

Possible Attacks on Nodes

To appreciate the challenge of securing a network, all the possible threats should be considered. Threats in UWSNs can be broadly classified into four categories: attacks on the data in the nodes, routing attacks, cloning attacks, and physical attacks. In normal WSN's since the sink is online for the whole time, it is feasible for the sink to detect most of the attacks in the network, but this line of defense is not possible in the case of UWSNs. Some possible attacks on the nodes are as follows [1]:

1. Attacks on Data: Since the network is unattended, the nodes have to save the data in their memory for a long time (i.e., until the next visit of the sink). This inability to offload the data makes the data an easy target for the adversary. The adversary can delete critical information or inject false measurement into the memory or modify the data.

2. Routing Attacks: UWSNs use multi-hop routing to transmit the data to the mobile sink (when the sink comes into the range of the node) or to send the data replicas and

Message Authentication Codes (MAC's) of a node to the other nodes. All the data transfer is done wirelessly, and this incurs routing attacks by the adversary. Some possible routing attacks [3] as follows:

(a) Spoofing: Spoofing is a direct attack against a routing protocol. The adversary can spoof, alter or replay routing information between the nodes. By doing this the adversary can create routing loops, extend or shorten service routes, generate false error messages and increase end-to-end latency.

(b) Selective Forwarding: General assumption when a message is forwarded through multi-hops is that the nodes will faithfully forward the received messages. In selective forwarding attack, malicious node behaves like a black hole, refuses to forward all the messages and drops certain messages. This attack can remain undetected as the malicious node suppresses only critical messages and forwards the rest to limit the suspicion.

(c) Sink Hole Attack: In the sink whole attack, all the trafic is attracted to a compromised node. This attack works by making the compromised node look attractive to the surrounding nodes. Sink whole attacks can enable other attacks like selective forwarding in the network.

(d) Sybil Attack: In Sybil attack, a node presents the identity of multiple nodes in the network. The Sybil attack targets the fault tolerant schemes such as multi-path routing, distributed storage, disparity, topology, replicas storage partitions. Sybil attack can be avoided by proper authentication and encryption techniques.

3. Cloning: Since the nodes in the network are deployed in hostile environments, they are vulnerable to capture and compromise. The attacker can copy the ID and data of the captured node into a new node and deploy it in the network. Node replication can severely disrupt the network performance. Data can be corrupted or misrouted. Node can send false reading to the sink. If the attacker can insert clones at specific segments of the network then it can gain access to a specific segment of the network.

4. Physical Attacks: In physical attacks, the attackers manually capture the nodes and reprogram them. The main advantage of this attack is quick and easy [4]. In UWSNs, the unattended and distributed nature of the network makes them highly susceptible to the physical attacks. Unlike the other attacks mentioned above, physical attacks can destroy the nodes permanently and the losses occurred are irreversible. Two types of physical attacks are possible:

(a) Jamming: In this attack the channel will be jammed with an interrupting signal. To jam a node or set of nodes in the network, a simple radio signal can be transmitted which interferes with the signals used by the other sensor nodes.

(b) Physical Tampering: Sensor nodes are vulnerable to physical harm or tampering. Tamper resistant hardware can be used to avoid this kind of attacks but it is not practical use such an expensive hardware for the entire size of the network.

II.LITERATURE REVIEW

Al-Mahmud, et al. [5] The advancement in wireless communications and electronics has enabled the development of low-cost sensor networks. The sensor networks can be used for various application areas (e.g., health, military, home). For different application areas, there are different technical issues that researchers are currently resolving.

The current state of the art of sensor networks is captured in this article, where solutions are discussed under their related protocol stack layer sections. This article also points out the open research issues and intends to spark new interests and developments in this field.

TC-BAC is proposed by Duan et al. [6] to allow access of a trusted node to a network. This model utilises trust to ensure that only legitimate nodes are permitted to join a WSN and then centrality degree2 to assess continually for risk of access. The concept of centrality degree is used to analyse the relations among the sensor nodes in the network for evaluation of risk. The trust records of other nodes' behavior are stored in each node for a local trust evaluation along with a centrality degree that represents its importance in the network. In the proposed model, the risk function mainly depends on the node's centrality degree and average trust degree in the network. The main contribution of this model is the introduction of trust and centrality degree attributes into RBAC engine to grant access control.

Maerien et al. [7] proposed an access control infrastructure based on RBAC for multi-party WSNs. In this model, an authorisation proxy acts as both the Policy Enforcement Point (PEP) and the Policy Decision Point (PDP). The proxy retrieves the user's current roles from the small database on sensor nodes to check and verify whether the user's role is sufficient for the access requests. The advantage of this model is that the proxy also monitors the behaviour of the users in the system to detect potential intrusion attempts and keeps a log for sensor node usage caused by the users. There is a lack of flexibility in the proposed infrastructure because the defined roles on sensor nodes only allow for certain evaluation of access rights.

Gaurkar et al. [8] proposed an access control model with intrusion detection for security in WSNs. They proposed a new framework for low-level intrusion detection at sensor nodes with access control. The main contribution of the proposed model is that it prevents a malicious node from joining the sensor network. The proposed model extends traditional access control to consider the problem of authorisation not only at the time of access to a resource. The concept of Reference Monitor (RM) is used to enforce data access but there is no detailed information of how the access control is performed in the proposed model.

Chatterjee et al. [8] proposed a user access control scheme for Wireless Body Area Network (WBAN). This schemes is used an ECC based crypto system to ensure that a particular legitimate user can only access the information for which he/she is authorised. This model uses an access list composed of a user identity, a user access privilege mask and a group identity for each user regarding data access. A user access privilege mask is a binary number where each bit represents specific information or services that can be

accessed by an authorised user. The group identity represents a unique number to identify a particular access group. This model is similar to Wang, Sheng and Li Model. The main difference is that ECC based crypto system is used in this proposed model.

III. TRUST MANAGEMENT FOR UWSN

Given the previously mentioned attacks that can affect the functionality of a UWSN, it may be argued that adopting a trust management system for UWSN does not bring enough advantages. But, trust is an important tool that can solve one of the intrinsic problems of WSN: the problem of uncertainty in collaboration. Besides, trust established between nodes can be used for other purposes beyond collaboration. Moreover, once the possible attacks against a trust management system are known, it should be possible to create more robust systems. In order to explain the suitability of trust for sensor networks, we will start with the concept of collaboration. All the members of a UWSN (sensor nodes and base stations) need to collaborate in order to provide the services of the network. Examples of these collaboration processes are sensing and routing. All sensor nodes use their sensing hardware in order to obtain physical information from the environment. Besides, every node behaves as a router, forwarding the physical information to the base station through other nodes. For assuring a successful collaboration, a node should be able to discover which nodes are more likely of accomplishing a certain task.

Trust Management Architecture

We have already discussed the importance of trust for UWSN and why we need trust management systems for these types of networks.

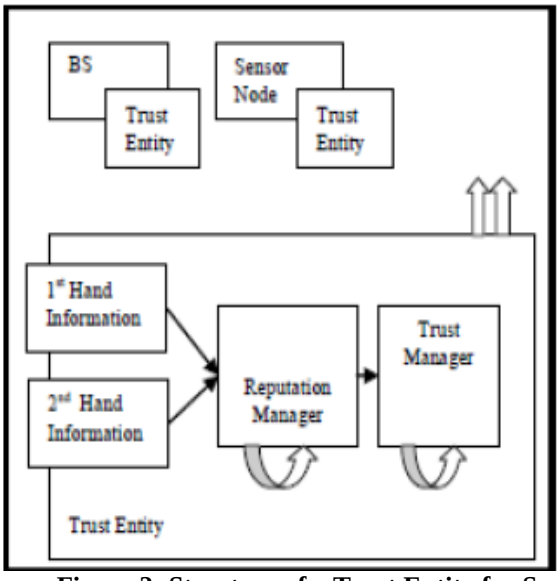

Figure 2: Structure of a Trust Entity for Sensor Networks

The architectures considered in the literature for solving the challenge of managing trust relationships differ depending on the underlying problem. For sensor networks, it is necessary to have a lightweight distributed architecture that tries to assure coverage of the whole network. This architecture must be "behaviour-based" in order to react to the events that may occur during the lifetime of the network. These requisites are given by the decentralized nature of UWSN and its specific characteristics and constraints. An important element of any trust management system is the trust entity. This entity is in charge of obtaining, calculating and maintaining reputation and trust values.

IV. PROPOSED SOLUTIONS

Different authors have provided a number of solutions to secure Directed Diffusion against some of the attacks mentioned above. VijayRaman Kumar et al. [8] have proposed a solution to secure Directed Diffusion using a key management protocol called LEAP (Localized Encryption and Authentication Protocol). Different keys have been used to provide various levels of security in this approach. Each node shares a pair-wise key with all its neighbours for secure communication between them. All the nodes in the sensor network share a Global key with the base station which is used by the base station to encrypt the interest message and by other nodes to decrypt the messages from the base station. Each node has also a unique individual key which is used for secure communication between the node and the base station. The base station verifies the messages sent by this node using this key. The approach taken by the authors can secure Directed Diffusion against cloning, flow suppression attacks but cannot effectively work against selective forwarding attack as the adversary can drop an encrypted packet at its will.

The main phases of the protocol are:

- Secret-key setup and broadcasting phase
- Interest propagation phase
- Path establishment and reinforcement phase
- Data-event delivery and authenticated acknowledgement delivery phase
- Disclosed key and buffered ACK-packets authentication phase

Trust model: A node Ni receives observations about another node Nj from all of its neighbors, and combine all the recommendations along with its direct observation to estimate the trust on N_j. The weight age given to direct observation is more than the recommendations. So, Ni will tend to trust its experience more than others' recommendations. Hence, if a malicious node tries to propagate bad reputation about legitimate nodes or tries to propagate good reputation about malicious node, it cannot drastically change the opinion of the observers. Thus, our trust model is effective against good mouthing and bad mouthing effect.

The step-by-step procedure is listed in the next section.

ALGORITHM

Data structures maintained at each node:

1. Trust of the neighbours of node i at nodei (Trustj : jϵ Neighbouri)
2. View of the neighbours of node i at nodei {(bj,dj,uj : jϵ Neighbouri)}
3. (α,β) for all neighbours. Initially, (α,β) =(1,1)
4. Default trust value of the neighbours T> θ
5. Malicious_list containing the node_ids of the malicious nodes detected by nodei

Sink_code() listed below is executed at the sink.

Sink_code()

1. The sink broadcasts **INTEREST** to the non-malicious neighbours.

2. If msg_received== **EXPLORATORY_DATA**

2.1. Forward **POS_REINF** to a downstream node.

3. If no **DATA** message received

3.1. Forward **NEG_REINF** to the node that was previously reinforced.

3.2. Send **POS_REINF** to another neighbor with highest trust

IntermediateNodes_code() algorithm is executed at the sensor nodes that behave as intermediate node w.r.t the message that it received.

IntermediateNodes_code()

1. If msg_received== **INTEREST** && sender!=malicious

1.1. Broadcast **INTEREST** to non-malicious neighbours

1.2. Set up gradient with the sender

2. Else discard

3. If msg_received== **EXPLORATORY_DATA** && sender!=malicious

3.1. Forward **EXPLORATORY_DATA** to the non-malicious upstream nodes

3.2. Send **ACK** to the downstream nodes

4. Else discard

5. If msg_received== **POS_REINF**

5.1. Forward **POS_REINF** to the downstream node with highest trust

5.2. Send **ACK** to the upstream node

6. If msg_received== **DATA** && sender!= malicious

6.1. Send **ACK** to the sender

6.2. Forward **DATA** to the node from which it received **POS_REINF**

7. Else

7.1. Send **NEG_REINF** to the sender

7.2. Send **POS_REINF** to another downstream node with the highest trust

8. If msg_received== **NEG_REINF**

8.1. Forward **NEG_REINF** to the node that was previously reinforced

9. If msg_received== **ACK** || timeout occurs

9.1. Update_beta()

9.2. Update_view()

9.3. Calculate_cumulativeBelief()

9.4. Calculate_Trust()

10. If msg_received== **VIEW** && sender!=malicious

10.1. Calculate_cumulativeBelief()

10.2. Calculate_Trust()

11. Else discard

V.EXPERIMANT RESULTS

First an example is cited for better understanding of the protocol. Then the results are discussed. As each node forwards packets to an upstream node, it waits for an ACK from the upstream node. The upstream node on forwarding the received packet to its subsequent upstream node sends an ACK packet to the downstream node. On receiving ACK from the upstream node or in case of timeout, the observing node updates its trust on the upstream node according to the algorithm. Here, node 27 which is the source generates a packet and forwards it to its neighbour node 2 and waits for an ACK from node 2 on successful forwarding of the packet by node 2. Node 2 sends an ACK to node 27 on successful forwarding of the packet and it does not send any ACK to the sender when it does not forward the packet. Based on receiving ACK from node 2 or in case of timeout, node 27 evaluates its trust on node 2.

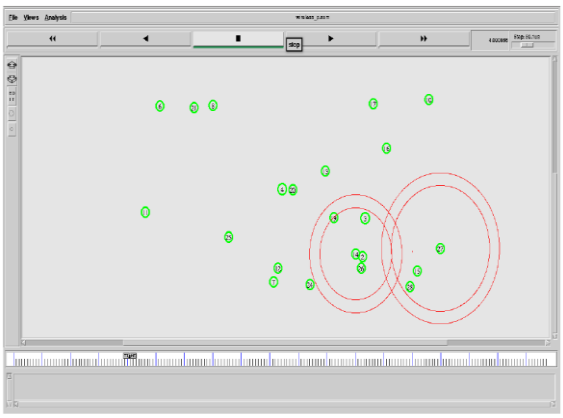

Figure 3: Packet forwarding by the source to its neighbour

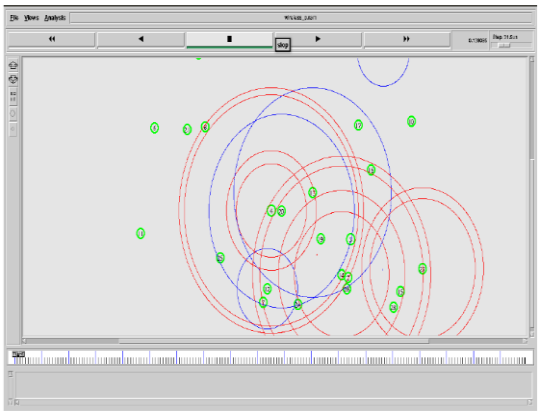

Figure 4: ACK sent by node 2 to node 27 on forwarding the received packet

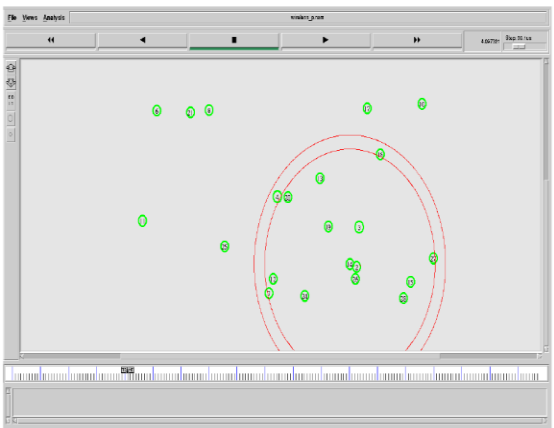

Figure 5: Packet dropped by node 2 and no ACK sent to node 27

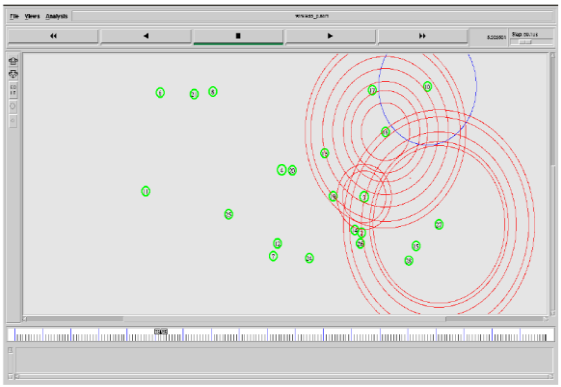

Figure 6: Alternate neighbour selected for packet forwarding

Since node 27 has detected node 2 as malicious, therefore it stops transactions with it and forwards its packets to node 16. The following graph shows the result of how the proposed scheme works better than without scheme. The graph shows the comparative performance of the Directed Diffusion protocol with and without the proposed scheme. The performance metric considered is Packet Delivery Ratio. The packet delivery ratio is defined as the ratio of number of data packets received at the destination over the number of data packets sent by the source [7].

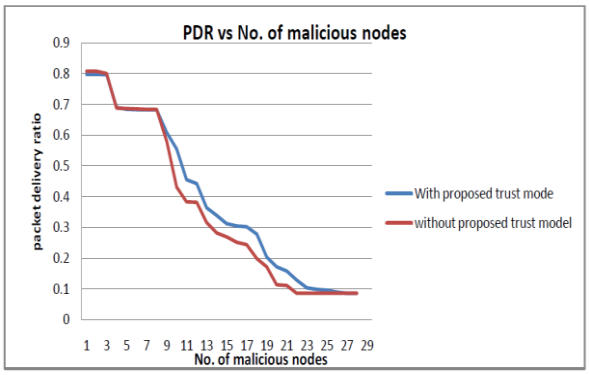

Figure 7: Variation of packet delivery ratio with no. of malicious nodes

Here, we can see that the packet delivery ratio of the Directed Diffusion protocol with the proposed scheme is greater than without the scheme. Initially, the performance of the Directed Diffusion protocol with and without the scheme is similar till there are about 10% malicious nodes in the network. But, from thereon, Directed Diffusion with the proposed scheme performs considerably better till there are about 89% malicious nodes in the network. This is because, after detection of malicious nodes, the legitimate nodes refrain from any transactions with them. Hence, the packet delivery ratio of the proposed scheme is greater. However, when all the nodes in the network become malicious then the performance of Directed Diffusion with or without the scheme is similar.

VI.CONCLUSION

In this work, we have proposed a trust and reputation based secure Directed Diffusion routing protocol for wireless sensor network. However this trust model so developed can be readily extended for other routing protocols in order to deal with the problems of selective forwarding, good mouthing and bad mouthing. It is assumed that malicious nodes send acknowledgement to the sender when it forwards the packets received. We have not considered the case when it sends acknowledgement even when it drops the received packets.

VII.REFERENCE

[1]. A. S. S. Mateus, C. B. Margi, M. A. S. Jr., C. C. F. P. Geovandro, B. T. de Oliveira, \Implementation of Data Survival in Unattended Wireless Sensor Networks Using Cryptography," in Proc. IEEE Conf. on Local Computer Net- works (LCN), pp. 961,967, 2010.

[2]. M. Sirivianos, D. Westho_, F. Armknecht, J. Girao, \Non-Manipulable Aggregator Node Election Protocols for Wireless Sensor Networks," in Proc. Int. Symp. on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt), pp. 1-10, 2007.

[3]. M. Bellare, S. Miner, \A Forward-Secure Digital Signature Scheme," in Proc. Annual Int. Cryptology Conference (CRYPTO), Lecture Notes in Computer Sci- ence, vol. 1666, pp. 431-448, 1999.

[4]. W. Du J. Deng, Y. S. Han, P. K. Varshney, \A Witness-Based Approach for Data Fusion Assurance in Wireless Sensor Networks" in Proc. IEEE GLOBECOM, pp. 1435-1439, 2003.

[5]. S. Capkun, M. Cagalj, M. Srivastava, "Secure Localization with Hidden and Mobile Base Stations," in Proc. IEEE INFOCOM, 2006.

[6]. Y. Chen, W. Trappe, R. P. Martin, "Attack Detection in Wireless Localization," in Proc. IEEE INFOCOM, 2007.

[7]. S. Hussain, F. Kausar, A. Massod, "An Efficient Key Distribution Scheme for Heterogeneous Sensor Networks," in Proc. Int'l Conf. on Wireless Communications and Mobile Computing (IWCMC), 2007.

[8]. Hajime Kimura, K.M. and Shigenobu Kobayashi, "Reinforcement Learning in POMDPs with Function Approximation", ICML, Vol. 97, pp. 152-160, 1997.