A Framework to Prevent Mobile Sinks Accessing by Unauthorized Nodes in WSN

Abhishek Pandey
Indian Institute of Information Technology, Allahabad.

Neeraj Kumar
Indian Institute of Information Technology, Allahabad.

R. C. Tripathi
Indian Institute of Information Technology, Allahabad.

ABSTRACT

Due to resource constraint nature of sensor nodes, the network suffers by computation and security problems. These nodes create a wireless sensor network that used sink stable or mobile as per required applications. Therefore, various traditional security techniques of the traditional networks are not possible to be applied on this network. To overcome the security problem in this ad-hoc or wireless sensor network, the current model has proposed a framework known as sink security model to secure mobile sink node with the help of an algorithm. This algorithm provides ability to mobile sink for deciding the correct situation about data reception using the past record.

Keywords

Security threats, adversary, NS-2, Mica2, Mica2Dot.

1. INTRODUCTION

Past few years have witnessed many examples using wireless sensor network's use in very sensitive areas like military surveillance applications, real time monitoring in civil engineering, human tracking or health monitoring. In some specific applications of WSN, security plays a prime role for the desired results, but in the WSN, there are several difficulties to implement the security as compare to the wired networks due to the limited capability of the devices along with resource and medium limitations. In this paper, a framework has been proposed with an algorithm to be applied on the mobile sink with the help of a small algorithm performed on the source nodes. According to this framework, the mobile sink makes a wall of trusted node in its surrounding.

For assumed defense applications, mobile sink needs to be secure with security approach for it. Proposed solution considers mobile sink with a normal mote but it may be a more powerful device. The importance and vulnerability of sink node invites attention of attackers, who can corrupt the network through control over the mobile sink. Attackers want to harm mobile sink by sending data from unauthorized device. Attackers can attack through jamming, through corruption in the message or through other possible attacks that can use identity of existing node of network. Here

The second section of paper provides the related work done using the trust and reputation for the security in WSN.

2. RELATED WORKS

Shen et al. proposed a protocol with one-way key chain that has been derived using hash function [6]. Through this protocol, they provide access control and authentication for various users using symmetric key with a central server. This scheme does not provide method to detect malicious nodes.

Zhou et al. proposed an access control protocol based on which authentication has been performed by handshaking between new nodes using Elliptic Curve Cryptography (ECC) [7], which is more energy efficient in his assumption. However, for sensor network it is also a costly method in terms of energy consumption.

Panja et al. proposed a role-based access control protocol for WSN, called RBASH [5], to provide multilevel security. Multilevel security is provided by the key assignment to different nodes based on their levels in such a way that a node at a higher level should be able to access data of nodes at lower level to which it is connected. Keys are distributed by arranging the whole network in form of hasse diagram. They proposed the model only for the homogeneous nodes not for the heterogeneous nodes.

Yang et al. proposed SCAF [4]. it uses a bidirectional evaluation scheme to secure the network on the Cluster head with Member node and member node with cluster head. In this, the cluster head and member node evaluates each other, judge their behavior, and calculates their data credit. After unsatisfactory credit cluster head assumes node is a malicious one whenever member node if found guilty to cluster head, they reports to the Base Station. They have not shown any energy consumption whenever it important is important for the WSN having mobile sink.

Crosby and Pissinou proposed a trust-based cluster-head election procedure for secure cluster formation [8]. They calculated reputation using the beta distribution of node's past behavior, considering the number of successful and unsuccessful interactions. They did trust calculation by taking the expectation of reputation.

Boukerche and Li proposed an agent based trust management scheme for WSN [9]. It assumes that clustered WSN is based on mobile agent system for trust maintenance with backbone. An agent launcher is assumed as a third party responsible to launch a mobile agent on request of node. This mobile agent was assuming as an attack resistant. However, this assumption might be wrong at some time.

Sudip et al proposed a model known as reputation management and role assignment scheme (RRAS) [1] for role-based access control based on reputation-based role assignment for wireless sensor networks. They considered scalability as a parameter for throughput in multilevel hierarchical network in WSN. RRAS requires a trusted component (TC) to be equipped with each node for reputation evaluation with node itself. These TCs has also assumed as a tamper resistant and cannot be attacked by adversary. In general, it is not possible.

TinySec [11] also has been used to provide the security in wireless sensor networks that is a very good approach to provide a security between links established between various nodes. However, it is not a complete model to secure a mobile sink node.

S.Zhu et al proposed a lightweight protocol [12] for the authentication between two hops, but this was not able to secure a hop against the hello flood attack and warm-hole attack so it is not useful to secure the mobile sink.

Shahabuddin et al proposed architecture to secure mobile sink likely much related with the problem statement [10], hence this described here in detail. They propose two-wall secure mobile sink node architecture for securing mobile sink in wireless sensor network. His approach defines first level of protection by selecting mobile sink neighborhood nodes as the only nodes allowed to communicate with mobile sink node. These nodes have chosen from the neighborhood of mobile sink node and form the inner protection layer. This defines a measure of trust as a trust level and associates it with every neighbor of mobile sink node. The trust level maintain by each mobile sink node and acts as a priority variable in the selection of its layer-1 nodes. The second level of protection is an outer layer of nodes protecting the inner wall. These second level nodes have chosen from neighbors of the inner layer nodes. These layers works like firewalls are still susceptible to attacks. This layer was able to deal with only DOS attack, spoofing and flooding attack.

Another approach [14] is used to maintain the trust of the node that was based on the trust value estimated on the mean value of reading given by the neighbor node to any node. With this, drawback is that in this case it is not sure that reading given by the neighbor node is correct.

G.zhan [3] proposed a trust model to evaluate the trustworthiness of nodes in hierarchical wireless sensor networks, focusing on data integrity. However, mobile sink security model focuses on trust maintenance to secure the mobile sink.

3. PROPOSED SOLUTION

The proposed solution has assumptions that Network uses the honey node concepts [2] to secure the mobile sink. Proposed solution makes a wall to maintain the security with the help of algorithm MACBAT that has been applied on the mobile sink node. Here mobile sink maintains a database about the id as nid of sensor nodes with the corresponding secret keys to generate the corresponding MAC and location of the deployed node to choose the node with high trust in the particular region. To make the wall of trusted node it only checks the trust at first time for the pre- decided period.

To check the trust of wall, proposed solution uses the approach for checking the trust of every node with the help of MAC received from the source node with the MAC generated at the mobile sink with the predefined key that is the shared secret with the particular node. To generate the MAC mobile sink uses the X-OR encryption technique defined by Mihir, Joe, Fillip [13] for the CBC MAC, but solution is not uses the chaining rule for transaction in a defined time slot, solution uses only one step to generate the MAC. The Proposed solution assumes that At the both end, on mobile sink or source node, Every node has a secret key that is shared with mobile sink node and secret from the all other node and from the outside of the world. In the proposed solution, assumption is that in the network message of fixed length are being sent. For fixed length message there is a technique to generate a MAC value through the XOR operation with a shared secret key. According to proposed solution, the security will be maintained by two operations, one will do work at the source end and another one will be performed at mobile sink end, According to mobile sink security model at the source end the MAC must be generated and sent to mobile sink with message along with the node-id.

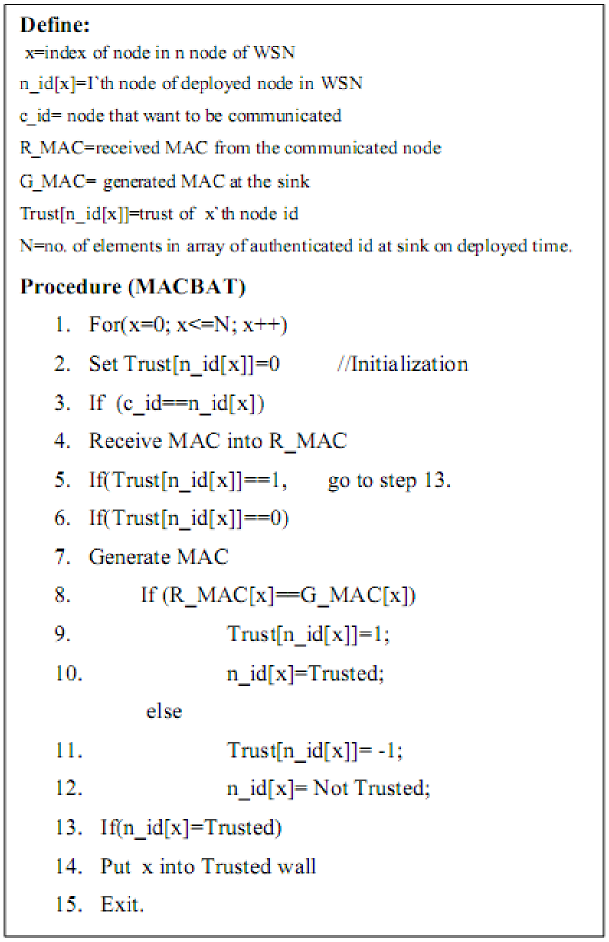
At mobile sink end, mobile sink improves its history using the MACBAT just as the updating table given below:

Condition	Initial Past History	If MAC equal	MAC not equal
History(Value)	0	1	-1

Table 1. History Updating Table

Here the 0 has meaning that the source’s history is currently in the initial condition which means there is not any trust check have been completed for the particular source or MACBAT is not performed with this source node. Whenever just after successful completion of MACBAT the history updated to 1, means both MAC are matched so history is 1 ,And when a MAC is not matched or node is not trusted history just goes to -1 and node is just fall in un-trusted node, means not trusted for the further communication.

MACBAT: The proposed solution assumes that there is a predefined unique shared secret key between source and mobile sink for every source node. With this key, the source generates a MAC and transmits it to mobile sink with the message and mobile sink compares it with generated MAC. According to proposed solution mobile sink updates its past history on the bases of this MAC.



Define:

x=index of node in n node of WSN

n_id[x]=I`th node of deployed node in WSN

c_id= node that want to be communicated

R_MAC=received MAC from the communicated node

G_MAC= generated MAC at the sink

Trust[n_id[x]]=trust of x`th node id

N=no. of elements in array of authenticated id at sink on deployed time.

Procedure (MACBAT)

```
1.  For(x=0; x<=N; x++)
2.  Set Trust[n_id[x]]=0        //Initialization
3.  If (c_id==n_id[x])
4.  Receive MAC into R_MAC
5.  If(Trust[n_id[x]]==1,     go to step 13.
6.  If(Trust[n_id[x]]==0)
7.  Generate MAC
8.      If (R_MAC[x]==G_MAC[x])
9.              Trust[n_id[x]]=1;
10.             n_id[x]=Trusted;
        else
11.             Trust[n_id[x]]= -1;
12.             n_id[x]= Not Trusted;
13. If(n_id[x]=Trusted)
14. Put x into Trusted wall
15. Exit.
```

Figure: 1 MACBAT

Here the time complexity, for the MACBAT in worst case will is just O(n).

4. IMPLEMENTATION

In the implementation, solution assumes the Mica2 mote for mobile sink node and Mica2dot for the source nodes designed by the Crossbow Technology. The proposed solution recommends third generation Mica2 Mote that is designed especially for Embedded Sensor Networks and has 1 Year Battery lifetime on AA in Sleep Mode. As a source node for deployment of a network, the solution assumes mica2dot for Temperature and Environmental Monitoring and Mica2 in case where cost is not a case. In general, where cost is a case, solution recommends Mica2dot due to its low size 25 mm, routing capability with mica2 compatible Multi-channel Radio Transceiver used. The MICA2DOT communicates with base stations that use the MICA2 radio module.

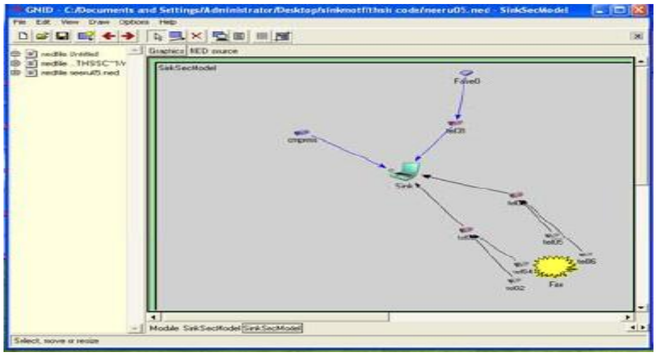


Figure2: Network model to work

To the implementation of the given problem statement (figure 2) the solution assumes that there are ten sensor nodes are deployed for the implementation. In this implementation one is the fully fake node sending data through trusted node to mobile sink and one is a node that has the id of original deployed node of network but not has the secured secret key of the deployed node. There are four correct node that are sending the data to mobile sink through the trusted node.

The implementation of proposed solution has been performed using the ns-2 simulator to simulate the model with language Tcl as described in the next section. To plot the result over energy consiomption and the connection two plotting tool have been used, GNUPLOT and XGRAPH as per requirement to show.

Energy Consumption at sink: The simulations have been implemented for energy conservation on given conditions:

1. Energy consumption at mobile sink without security approach to save mobile sink

2. Energy consumption at mobile sink with existing security approach given by shahabuddin [10]

3. Energy consumption after the use of mobile sink security model to secure mobile sink

In its consideration the channel is wireless, radio propagation mode two ray ground, network interface is wireless physical, link layer is LL with Mac 802.11, in this the consideration about the antenna assumed as unidirectional, here the protocol for routing is considered a AODV applied for the node 10, 7 and 8 in simulating for the different scenario.

✓ Without any security approach:

In this case, the full energy of mobile sink node is going to be loose in just before 15.7 second of the simulation, whenever mobile sink has 1-joule energy at mobile sink.

The figure 3a shows the energy consumption at mobile sink node without any security approach.

✓ With existing model

In this model, energy consumed at mobile sink in just 19.4 second, in the simulation of 20 second.

The figure 3b shows the energy consumption at mobile sink node with an existing security approach defined by shahabuddin [10].

✓ With mobile sink Security model:

The figure 3c shows the energy consumption at mobile sink node with proposed security model using the MACBAT algorithm on mobile sink.

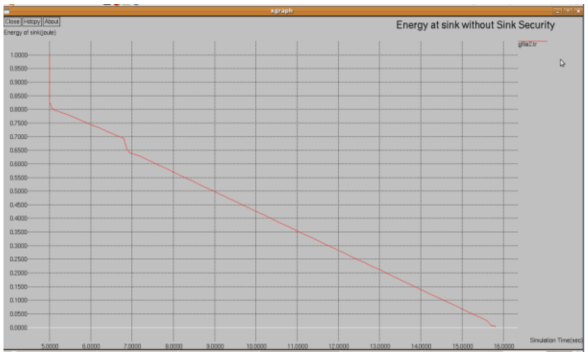


Figure 3a Energy consumption without any Model at mobile sink

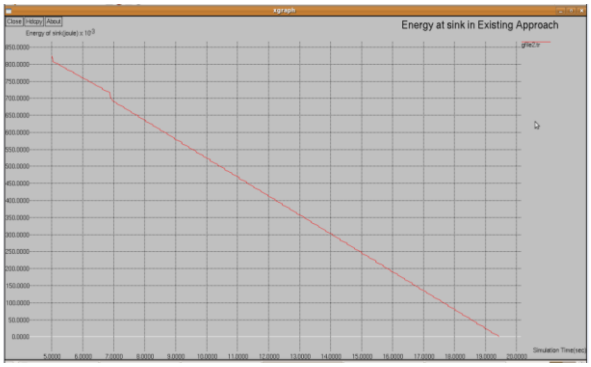


Figure 3b Energy consumption with Existing Model at mobile sink

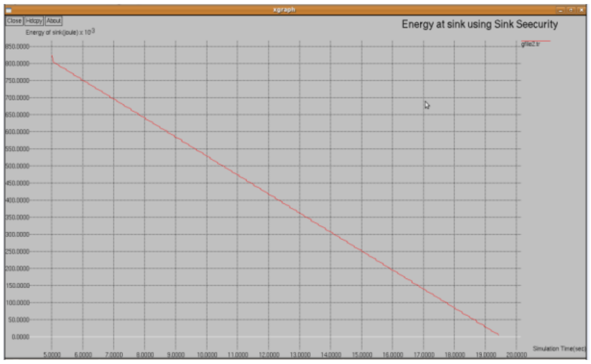


Figure3c Energy consumption with sink Security Model at mobile sink

Connection between nodes:

Without apply mobile sink security: Without applying any security model, a fake node can transfer the data so the connection will be look like as:

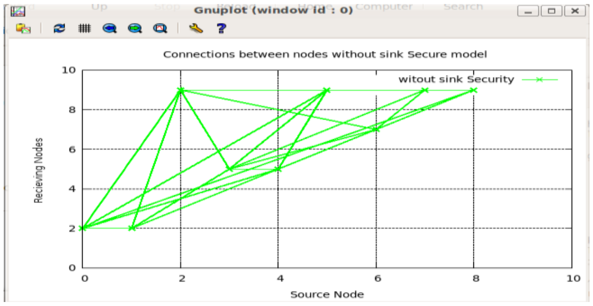


Figure 4a Connection between nodes without Mobile sink Security Model

After apply mobile sink security: After the use of mobile sink security model there is no possibility to connection of fake node with mobile sink as per assumption, so the connection will look like as per snapshot given below:

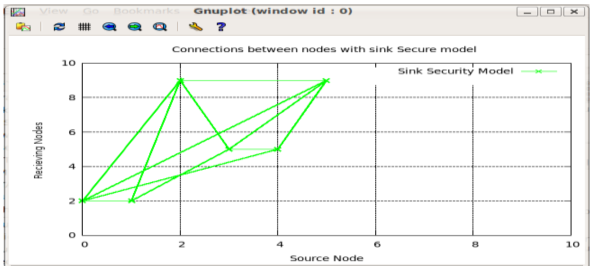


Figure 4b Connection between nodes with Mobile sink Security Model

In this implementation, considerations are that mobile sink is not communicating with the unauthorized due to the use of algorithm of model.

5. ANALYSIS

Time Complexity for the MACBAT: In the MACBAT step 1 and 2 will take N iterations to finish, so statement executions will be 3N+1. That is directly proportional to N the time complexity here will be O(n). Whenever step 3 and 4 also will go to take time complexity in worst case O(n). For step 5 to 15 all steps taken the time complexity of O(1) because every step only runs in linear time. So finally here the time complexity for the algorithm in the worst case is O(n). It means our algorithm runs at linear time.

Failure Probability of the Wall: To analyze this probability method uses the basics of probability to support paper work. Consider a sensor network with M motes excluding the mobile sink node, in which Mc has chosen trusted node to maintain wall-using MACBAT. If P is the probability to break the wall i.e. break on single node is enough to break the wall. Only one node break in a wall from the Mc nodes can break the wall, so the probability to break the wall without using key, assumes as Pw :

$$Pw = 1 / Mc \qquad \ldots 2$$

In addition, we know a node can break only in situation when the key of node is known, so probability to break the key assumed Pk then,

$$Pk = \frac{1}{Base^{Key\ size\ of\ key}} \qquad \ldots 3$$

If the chosen keys of node is different and mobile sink has a key ring then the probability to break the wall with a single node will be

$$Pwb = Pw * Pk \qquad \ldots 4$$

$$P=Pwb=1/Mc*\frac{1}{Base^{Key\ size\ of\ key}} \qquad \ldots 5$$

Advantages: The advantage behind framework is that it secure mobile sink in better way than the existing approach because here the MAC verification is performed with different keys for every node. This model has a possibility to increase the security after applying encryption Algorithm to transfer cipher text in place of plain text. This model minimizes delay in compare with existing approach due to one hop communication between the authenticated node and mobile sink.

Disadvantages: For security in applications, it demands a costly deployment to deploy powerful mote such as Mica2.

6. CONCLUSION & FUTURE WORK

Proposed solution is a new and flexible framework to secure mobile sink node or to cluster-head because it has aggregated data for the further processing that make them a vulnerable and important for the adversary. The algorithm MACBAT suggested in the framework is an economically good algorithm, which is running in linear time. i.e. time complexity is O(n) in the worst case. Therefore, it will take the least cost for processing. Energy consumption at mobile sink due to this model is not a matter being worried because it is not an energy consuming process as compared with existing approach as per result seen in chapter 6. This model provides intelligence to mobile sink to decide whether a node is trusted or not. Now mobile sink prevents itself from unauthorized access by any un-trusted node or from any adversary.

The Framework to secure mobile sink is flexible in terms of encryption algorithms to generate a MAC in used algorithm that can be change as per requirement of application, so in this model MAC can be hard to harder as per user's requirement as per application

7. REFERENCES

[1] S. Misra, A. Vaish, "Reputation-based role assignment for role-based access control in wireless sensor networks", journal of Computer Communications of Elsevier (2010), 2010.02.013.

[2] S.Misra, S.K.Dhurandher,A.Rayankula and D.Agrawal, "Using Honeynodes for defense against jamming attacks in wirelessinfrastructure-basednetworks"; Computers & Electrical Engineering Volume 36, Issue 2, Pages 367-382, Wireless ad hoc, Sensor and Mesh Networks, March 2010.

[3] G.Zhan,W.Shi and J. Deng, "Poster Abstract: Sensor Trust - A Resilient Trust Model for WSNs" SenSys'09, November 4–6, 2009, Berkeley, CA,USA.ACM 978-1-60558- 748-6

[4] W.C. Yang, Y.Y. Zhang, K.B.Kim, J.H.Kim, M.S.Park, "SCAF: a secure cluster-based architecture formation scheme for wireless sensor network", in: Proc. 4th IEEE International Conference on Circuits and Systems for Communications (ICCSC 2008), May, 2008, pp. 843–847..

[5] B.Panja, S.K. Madria, B.Bhargava, "A role-based access in a hierarchical sensor network architecture to provide multilevel security", Computer Communications 31 (4) (2008) 793– 806.

[6] Y.Shen, J.Ma, Q.Pei,"An access control scheme in wireless sensor network", in: Proc. 4th IFIP International Conference on Network and Parallel Computing Workshops(NPC 2007), Dalian,China, September, 2007, pp. 362–367.

[7] Y. Zhou, Y. Zhang, Y. Fang, "Access control in wireless sensor networks", Ad Hoc Networks 5 (1) (2007) 3–13.

[8] G.V.Crosby, N. Pissinou, "Cluster- based reputation and trust for wireless sensor networks", in: Proc.4th Consumer Communications and Networking Conference (CCNC 2007), January, 2007, pp. 604–608.

[9] A. Boukerche, X. Li, An agent-based trust and reputation management scheme for wireless sensor networks, in: Proc. IEEE Global Telecommunications Conference, 28 November–2 December, 2005, pp. 1857–1861.

[10] S.Muhammad, Z.Furqan andR.K.Guha, "Wireless Sensor Network Security: A Secure Mobile sink Node Architecture". In Proceedings of the 24th IEEE International Performance Computing and Comm. Conference (IPCCC), Arizona, USA, April 2005,pp.371-376.

[11] C. Karlof, N. Sastry, and D.Wagner, " tinySec: A Link Layer Security Architecture for Wireless Sensor Networks," in Second ACM Conference on Embedded Networked Sensor Systems (SenSys 2004), Nov. 2004.

[12] S. Zhu, S. Xu, S. Setia, and S.Jajodia,"LHAP: A Lightweight Hop-by-Hop Authentication Protocol for Ad-Hoc Networks", Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops (ICDCSW'03) , May 2003.

[13] M.Bellare, J.Kilian, F.Rogaway, "The security of cipher block chaining message authentication code",crypto94 proceedings, Lecture note in computer science vol. 839, 1999.

[14] C.Burattiy, F.Cuomo, S.Della, Luna, U. Monaco, J.Orrissx, R.Verdoney; "Optimum Tree-Based Topologies for Multi-Mobile sink Wireless Sensor Networks Using IEEE 02.15.4"