Anomaly Detection in the Wireless Sensor Networks with Triple Performance Metrics

I. Gayathri Devi,
Asst.Professor
Cse Department,
Pragati Engineering College,
Surampalem, Kakinada, Ap, India,

G. Kumari,
Asst.Professor
Cse Department,
Pragati Engineering College,
Surampalem, Kakinada, Ap, India,

***Abstract*— this paper is based on the behaviour of sensor nodes along with performance metrics in wireless sensor networks. In this, the information collected and identity to the nodes are considered to prevent from malicious nodes along with effective use of capacity and lifetime of nodes. The behaviour profiles of authorized nodes and intruder are collected and then make a match of the behaviours to identify the authorized user. But this approach may arise misfeasor class of intruder. So, to resolve this, an extension is made in this paper that the intruder can be identified and ejected from the network using a triple-stage metrics without data aggregators. One is node-based authorization technique, in which the identity among the nodes is verified using HMAC algorithm. Second is link-based integrity technique, in which each message is sent over double path in a encrypted manner by using the random key for encryption to provide confidentiality and nonce value is added to the each message in order to prevent from replay attacks. Third, is to calculate the metrics for network capacity and network lifetime among the nodes using SLP-PA approach to retain the energy of the nodes in the network requirement. Where, each node to be utilized in an efficient manner to forward the packets across the network. Such that, the total throughput can achieve an optimal point subject to common lifetime requirement on all nodes without requiring any energy reservation during each iteration.**

***Keywords* — Wireless sensor networks, Behaviour anomaly, Intruder, node capacity, node lifetime, authentication, confidentiality, integrity, replay attacks.**

I. INTRODUCTION

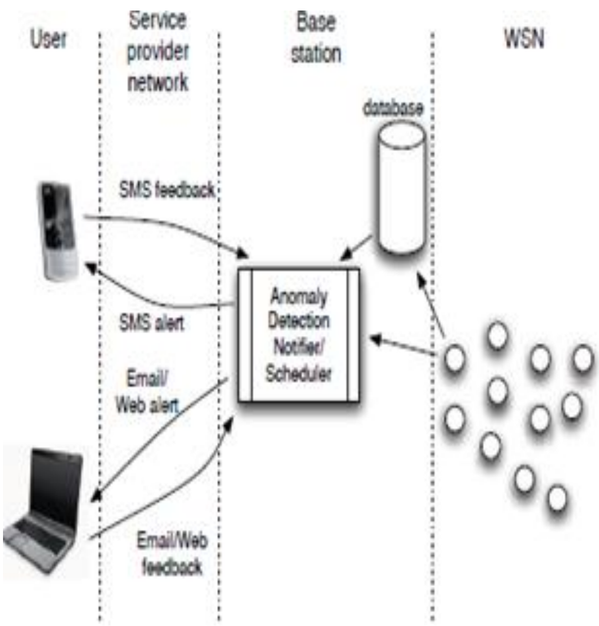
Wireless sensor networks composed of thousands of highly integrated sensor nodes hold the promise of sensing that is far superior, in terms of quality, robustness, cost and autonomous operation. A sensor network consists of sensor nodes and one or more base stations. Sensor nodes generate, process, and forward data (via intermediate sensor nodes) to base stations. The challenges in the design of sensor networks are the efficient utilization of resources available to sensor nodes such as scarce bandwidth, limited energy supply and the security issues.

A WSN is a special type of network. It shares some commonalities with a typical computer network, but also exhibits many characteristics which are unique to it. Wireless sensor networks processing sensitive data are facing the risks of data manipulation, data fraud and sensor destruction or replacement. The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehaviour of nodes.

The design and implementation of secure WSNs must simultaneously address several difficult research challenges. First, wireless communication among the sensor nodes increases the vulnerability of the network to eavesdropping, unauthorized access, spoofing, replay attacks. Second, the sensor nodes themselves are highly resource-constrained in terms of limited memory, CPU, communication bandwidth, and especially battery life.

The main aim of the duality performance metrics is to increase the network capacity and network lifetime over network requirement. To meet these criteria in an efficient manner, a SLP-PA approach has been proposed. For a wireless sensor network, where each node is provisioned with an initial energy. For each node we solve an LP problem, to calculate the maximum rate at each level based on the available energy for the remaining nodes, until all nodes use up their energy. This is called “Network Capacity”. We call this naive approach “Serial Linear Programming” (SLP).

Fig. 1. User Interaction with WSN anomaly detection [1]



For a wireless sensor network, where each node is provisioned with an initial energy. For each node we solve an LP problem, to calculate the maximum rate at each level based on the available energy for the remaining nodes, until all nodes use up their energy. This is called “Network Capacity”. We call this naive approach “serial Linear Programming” (SLP).

The main aim of the triple performance metrics is to increase the network capacity and network lifetime over network requirement with security related issues like authentication, confidentiality, integrity, reducing the bandwidth.

For sensor nodes above equation simplifies to

$$\sum_{\{j:(i,j)\epsilon A\}} fij \;+\; \sum_{\{j:(j,i)\epsilon A\}} fij \le Pi \qquad i\,\epsilon V$$

Assuming that base stations are responsible for data gathering the above equation simplifies to

$$\sum_{\{j:(j,i)\epsilon A\}} fij \le (Pi+Di)/2 \qquad i\ \epsilon\ Vs$$

$$\sum_{\{j:(j,i)\epsilon A\}} fij \;\le\; Pi \qquad i\epsilon\ Vb$$

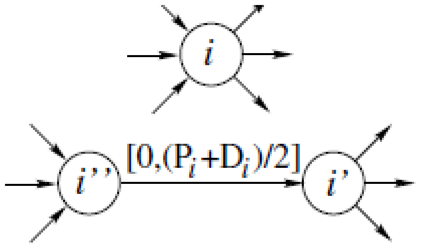


Fig. 2. Node Splitting

1) Split each node i ∈ V into two virtual nodes i1 and i2 .The input flow into node i corresponds to the input flow into node i2 and the output flow from node i corresponds to the output flow from node i1.

2) For each link (i, j) ∈ A ∪ A1, do the following: Replace (i, j) by a link (i1, j2) of the same cost and capacity.

3) Add a link (i2, i1) for each i ∈ V.

4) Set the cost of link (i2, i1) to zero and capacity to (Pi+Di)/2 for each node i ∈ Vs. The information generated by node i is assumed to be generated at node i2.

5) Set the cost of link (i2, i1) to zero and capacity to Pi for each node i ∈ Vb.

For Maximum lifetime:

$$Obj = Max\ l$$

$$\sum_{\{j:(j,i)\epsilon A\}} fij.\,\iota - \sum_{\{j:(j,i)\epsilon A\}} fij.\,\iota = Di.\iota \qquad i\epsilon\ Vs$$

$$\sum_{\{j:(j,i)\epsilon A} \left(\sum_{\{j:(j,i)\epsilon A\}} fkj.\,\iota - \sum_{\{j:(j,k)\epsilon A\}} fjk.\iota\right) = -\sum Di.\iota$$

$$\{i:i\epsilon Vs\}$$

$$\sum_{\{j:(j,i)\epsilon A\}} Tij.fij.\,\iota + \sum_{\{j:(j,i)\epsilon A\}} Rji.\ fij.\,\iota \le BEi \qquad i\epsilon\ Vs$$

$$0 < \iota$$

For Maximum Lifetime capacity:

$$Obj=Min\ q$$

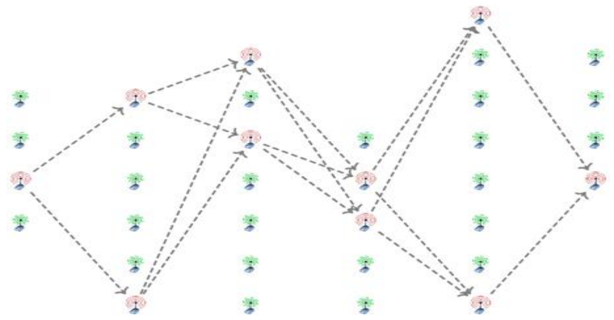
Due to the energy required for transmission over long distances, it is often a good idea to route data along a sensor network by making many hops over small distances instead of a direct transmission from a sensor to the sink node. However, such a solution has the disadvantage that an adversary can attack the network by gaining control over intermediate sensor nodes. The cryptography used by such devices is usually weak and can provide opportunities to reveal information sent or to manipulate them.

The following idea may be applied in order to make it much more difficult to carry out attacks. Instead of a single information path, each message is sent over a double path. This means that instead of a single ith node Ni we have two nodes: Pi and Ri. The encryption scheme has the following basic properties when processing a message M:

Pi+1 receives encrypted messages from Pi and Ri in order to compute its share of message M,Ri+1 receives different encrypted messages from Pi and Ri in order to compute its share of M.

The encryption scheme guarantees that corrupting either Pi or Ri reveals no information about M. Also, combining the shares from different stages of message processing gives no information about M as long as the adversary has only one share from each level of the path.

Fig. 3. Snapshot of a single routing path [7]



II. OBJECTIVE

The objective of this paper is to provide:

- Un-biased bit rate allocation with SLP-PA.
- Transfer of data with efficient utilization of bandwidth.
- Authentication for the Nodes.
- Confidentiality, integrity of the data transferred.
- Replay attacks are prevented.

III. PROBLEM FORMULATION

Wireless Sensor Networks are vulnerable to various types of attacks. These attacks are mainly of three types :

(i)**Attack on routing and self-evolving**: An attacker may change the routing of the intended users even though it retransmission on another path.

(ii)**Attacks on secrecy and authentication:** standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.

(iii)**Attack against service integrity**: in a stealthy attack, the goal of the attacker is to make the network accept a false data value. For example, an attacker compromises a sensor node and injects a false data value through that sensor node.

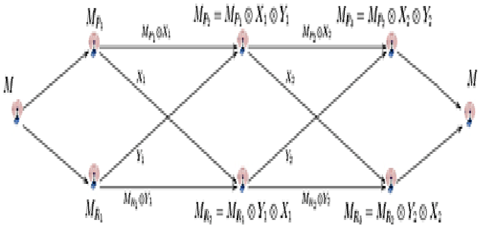
In these attacks, keeping the sensor network available for its intended use is essential.

Work Flow for Security issues:

- **Attack on routing:** A sensor network consists of many hops, over small distances instead of a direct transmission from a sensor to the sink node. However, such a solution has the disadvantage that an adversary can attack the network by gaining control over intermediate sensor nodes.

So, Instead of a single information path, each message is sent over a double path.The main point is that while it might be relatively easy to find and corrupt one of the nodes (say Pi) for this to be useful, the adversary must still find and corrupt the matching node Ri.

Fig. 4. Snapshot of double routing path[8]


M_{P_1}
$M_{P_1} \otimes X_1$
$M_{P_2} = M_{P_1} \otimes X_1 \otimes Y_1$
$M_{P_2} \otimes X_2$
$M_{P_3} = M_{P_2} \otimes X_2 \otimes Y_2$
M
X_1
X_2
M
Y_1
Y_2
M_{R_1}
$M_{R_1} \otimes Y_1$
$M_{R_2} = M_{R_1} \otimes Y_1 \otimes X_1$
$M_{R_2} \otimes Y_2$
$M_{R_3} = M_{R_2} \otimes Y_2 \otimes X_2$

- **Self-evolving:** At any time a node may negotiate with its predecessors and successors a change of the transmission key and redirect its duties to another node. Since these changes can be made independently and uniformly at random, the data path may evolve so fast as to make unfeasible any attempt at data analysis based on monitoring radio traffic.
- **Attacks on authentication, confidentiality and retransmission:** Initially a message created by the sender and attaches authentication, confidentiality, nonce value to protect from the attackers as follows:

The algorithm is stated as follows:

Process involved at the sender as follows:

1. For a message HMAC algorithm is applied which generates a MAC that is to be attached along with the message to gain authentication.
2. And, that message is compressed using a ZIP algorithm and encrypted using a random key which generates a compressed code to gain confidentiality
3. For the resulting code a nonce value is attached to show the freshness of the message.

This process is recovered at the destination as follows:

1. For the appeared code at the destination firstly check the nonce value to avoid replay attacks.
2. Secondly, decryption is applied to the code and decompression is applied to get the message along with MAC.
3. Thirdly, MAC is to be recovered by applying the HMAC algorithm for the message and check the calculated code and the appeared codes for a match.
4. If it matches then the sender is authenticated node.

Thereby, we can achieve the authentication, confidentiality, integrity, reduction of bandwidth by compressing the message and preventing the replay attacks by attaching the nonce values.

If the authentication fails for the node then that is identified and rejected its messages by using the anomaly detection notify.

IV. CONCLUSIONS

In this paper, presented a triple approach for protecting the wireless sensor network and also to maximizing the sum of rates of all nodes over an energy-constrained wireless sensor networks. A investigation is carried out on the authentication, confidentiality, replay attacks and routing attacks, that is to be prevented by using the algorithm which is proposed and redirecting its duties to the another node if the node is not working. There by, the attacker is detected by imposing security levels to the nodes if it fails then anomaly detection notify rejects its communication to the intended users.

ACKNOWLEDGMENTS

We thank to the Pragati Engineering College for giving support to the research work.

REFERENCES

[1] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[2] Hou, Y.T. Virginia Polytech. Inst. & State Univ., Bradley Yi Shi ; Sherali, H.D. Rate Allocation and Network Lifetime Problems for Wireless Sensor Networks

[3] A. Perrig, J. Stankovic and D. Wagner, "Security in Wireless Sensor Networks." In Communications of the ACM, Vol. 47, No. 6, June 2004, pp. 53-57.

[4] M. Bhardwaj and A. P. Chandrakasan, "Bounding the lifetime of sensor networks via optimal role assignments," in Proc. IEEE INFOCOM, New York, Jun. 23–27, 2002, pp. 1587–1596.

[5] Perrig, A., Stankovic, J., Wagner, D. (2004), "Security in Wireless Sensor Networks", Communications of the ACM, 47(6), 53-57.

[6] Shaikh,R.A.Dept. of Comp. Eng., Kyung Hee Univ., Suwon Jameel, H. ; d'Auriol, B.J. ; Sungyoung Lee ; Young-Jae Song ; Heejo Lee"Trusting Anomaly and Intrusion Claims for Cooperative Distributed Intrusion Detection Schemes of Wireless Sensor Networks "Young Computer Scientists, 2008. ICYCS 2008.

[7] Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp. 407-411.

[8] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no. 5, 2002, pp. 521-534.

[9] F. Anjum, D. Subhadrabandhu and S. Sarkar, "Intrusion Detection for Wireless Adhoc Networks." In Proceedings of the IEEE Vehicular Technology Conference, Wireless Security Symposium, October 2003, pp. 2152-2156

[10] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor networks: A survey," Comput. Netw. (Elsevier), vol. 38, no. 4, pp. 393–422, 2002.