A Stochastic Geometry Approach for Performance Analysis in Energy Harvesting Wireless Sensor Network

Thiyagarajan.G[1], Shyamala.J[2], Sunitha.T[3], Loganathan.A[4]

[1, 2, 3, 4]*Assistant Professor, Department of CSE, P. B.College of Engineering, Tamilnadu, India*

***Abstract*: Energy harvesting wireless sensor network (EH-WSN) is promising in applications, however the frequent occurrence of temporal death of nodes, due to the limited harvesting capability, presents a difficulty in meeting the quality-of-service requirements of the network. A Group of computers are connected to be able to exchange data and each node has a unique address. There is no bloom filter for carry provenance information to server for validate trusted node or not. We propose a provenance based encryption strategy whereby each node on the path of a data packet securely encrypts and also embeds provenance information within a Bloom filter (BF) that is transmitted along with the data. Here are three operations involved in this process are Active, Listening, Sleeping. In case of hackers attack the node, temporal death may occur. The AC motor will be turned on when the sensed value is above 40. When it is below 40 then the AC motor will be off. The temperature sensor is LM35 is used to detect the energy level of sensor Temperature sensor in the sense that provides temperature measurement through electric signal.**

***Index Terms*—Energy harvesting wireless sensor network (EH-WSN), temporal death.**

I. INTRODUCTION

Energy Harvesting Wireless sensor network (WSN) is formed by spatially distributed autonomous sensor nodes, which has the ability of self-configuring and self-organizing for the purpose of monitoring and collecting information. There is no bloom filter for carry provenance information to server for validate trusted node or not. In wireless sensor network each and every sensor have stored default encryption key for encrypt sending values, this key cannot change dynamically so hackers may possible to break the packet once know encryption key. Here we proposed a packet Bloom filter (IBF) provenance based encryption scheme. The problem of secure provenance transmission in sensor networks, and identifies the challenges specific to this context, the secure provenance based encryption scheme and device a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes.

A Packet is send to another node by using provenance based encryption strategy whereby each node on the path of a data packet securely encrypts and also embeds provenance information within a Bloom filter (BF) that is transmitted along with the data. There are three operations involved in this process are Active, Listening, Sleeping. In active mode, the node will process the sensor value. In listening mode, the node will wait for the sensor value from the previous node. In sleeping mode, the node will remain silent. No process will take place. In case of hackers attack the node, temporal death may occur. The metrics may involve Residual energy capacity, average queue length, blocking probability. Upon receiving the packet, the BS extracts and verifies the provenance information. We also send each provenance encryption key to server that allows the BS to detect if a packet drop attack was staged by a malicious node.

II.RELATED WORKS

2.1 Energy-Efficient Provenance Transmission

Trust evaluation frameworks use data provenance[3] along with the sensed data values to compute the trustworthiness of each data item. However, in a sizeable multi-hop sensor network, provenance information requires a large and variable number of bits in each packet, which, in turn, results in high energy dissipation with extended period of radio communication, making trust systems unusable. In an energy-efficient provenance transmission and construction scheme, which we refer to as Probabilistic Provenance Flow (PPF). Probabilistic Packet Marking (PPM) is an approach of IP traceback feasible for sensor networks.

2.2 Detecting Provenance Forgery and Packet Drop Attacks In Wireless Sensor Networks

Data they collect are used in decision-making for critical infrastructures. Data are streamed from multiple sources through intermediate processing nodes that aggregate information[5]. A malicious adversary may introduce additional nodes in the network or compromise existing ones. Therefore, assuring high data trustworthiness is crucial for correct decision-making. Data provenance represents a key factor in evaluating the trustworthiness of sensor data.

III. SYSTEM ANALYSIS

There is no bloom filter for carry provenance information to server for validate trusted node or not. In wireless sensor network each and every sensor have stored default encryption key for encrypt sending values, this key cannot change dynamically so hackers may possible to break the packer once know encryption key. In the existing Systen Block Cipher Function is used to encrypt the data which is the packet to forwarded.The disadvantages are

- There is no bloom filter for matching the sensor value.
- It does not handle the malicious nodes properly.
- Temporal Death is not archieved.

Here we proposed a novel method to securely transmit provenance with sensor data. This technique relies on in-packet Bloom filters to encode provenance. We introduce efficient mechanisms for provenance verification and reconstruction at the base station. In addition, we extend the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. The secure provenance based encryption scheme and device a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes. Each provenance have unique identification key and also random generate encryption keys that satisfies such security and performance needs. The provenance based encryption strategy whereby each node on the path of a data packet securely encrypts and also embeds provenance information within a Bloom filter (BF) that is transmitted along with the data. Upon receiving the packet, the BS extracts and verifies the provenance information. We also send each provenance encryption key to server that allows the BS to detect if a packet drop attack was staged by a malicious node.For more security we implement linear congruential generator. The Advantages are

- Malicious attacks are handled.
- Nodes can generate key values to transmit the sensed value to the next node
- Sensor network in provenance is addressed the security.

IV. SYSTEM DESIGN

The packet in a sensor is to design a provenance based data encryption Each provenance have unique identification key and also random generate encryption keys that satisfies such security and performance needs. We propose a provenance based encryption strategy whereby each node on the path of a data packet securely encrypts and also embeds provenance information within a Bloom filter (BF) that is transmitted along with the data. There are three operations involved in this process are Active, Listening, Sleeping. In active mode, the node will process the sensor value. In listening mode, the node will wait for the sensor value from the previous node. In sleeping mode, the node will remain silent. No process will take place. In case of hackers attack the node, temporal death may occur. The metrics may involve Residual energy capacity, average queue length, blocking probability. Upon receiving the packet, the BS extracts and verifies the provenance information. We also send each provenance encryption key to server that allows the BS to detect if a packet drop attack was staged by a malicious node.

4.1 User Level

This module contains sensor value encryption in every node. Here we give the sensor value and sensor number which has separate provenance value. We implement AES algorithm for cryptographic keys128, 192, and 256 bits block as input and output data.The packet is forwarded to one node to another node with the same data packet securely encrypts and also embeds provenance information

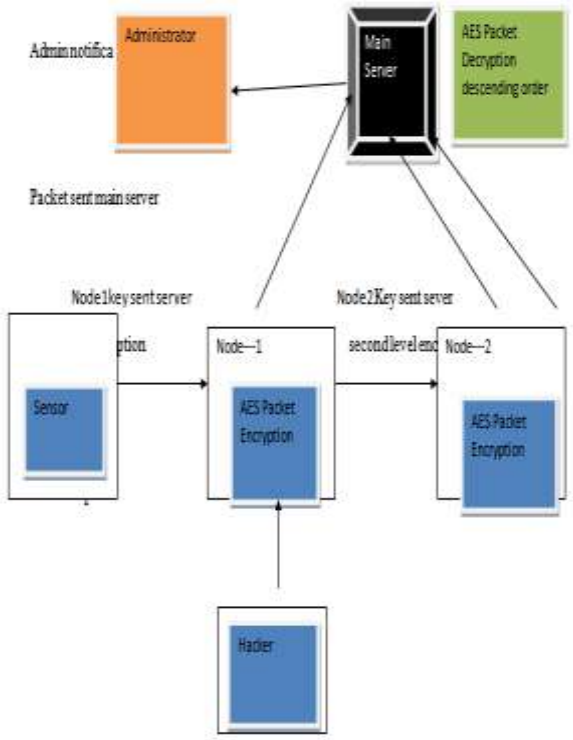


Fig 4.1 System Architecture

4.2 Packet Forwarding

The provenance based encryption strategy whereby each node on the path of a data packet securely encrypts and also embeds provenance information within a Bloom filter (BF) that is transmitted along with the data. There are three operations involved in this process are Active, Listening, Sleeping. Bloom filters have a strong space advantage over other data structures for representing sets, such as self-balancing binary search trees, tries, hash tables, or simple arrays or linked lists of the entries. Most of these require storing at least the data items themselves, which can require

anywhere from a small number of bits, for small integers, to an arbitrary number of bits, such as for strings.

4.3 Packet verification

The secure provenance based encryption scheme and device a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes. Each provenance have unique identification key and also random generate encryption keys that satisfies such security and performance needs. The provenance based encryption strategy whereby each node on the path of a data packet securely encrypts and also embeds provenance information within a Bloom filter (BF) that is transmitted along with the data. Upon receiving the packet, the BS extracts and verifies the provenance information. We also send each provenance encryption key to server that allows the BS to detect if a packet drop attack was staged by a malicious node.

4.4 Admin level notification

The packet of the sensed value is maintained provenance ,the original packet is forwarded to server.If provenance is not occurred the packet is hacked by the hacker.This notification is send to the admin from the server. Server that allows the BS to detect if a packet drop attack was staged by a malicious node. The AC motor will be turned on when the sensed value is above 40. When it is below 40 then the AC motor will be off.

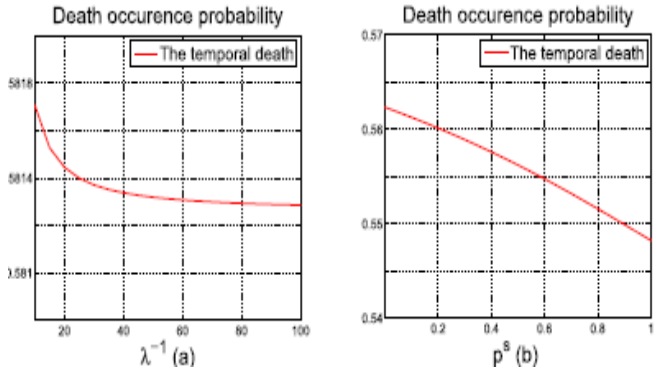
V. NUMERICAL RESULTS AND OBSERVATIONS

The dropping probabilities by means of the delay defined above. There are two types of dropping probabilities: the dropping probability due to energy depletion, which is denoted by *DPen* and the dropping probability due to channel error, which is denoted by *DPch*. Given the initial state of $\{(Xdr, \phi dr)\}$ is (x, i), we express the following two events by the first passage time.

• $\{$the given packet is dropped due to energy depletion$\} = \{\tau X(x) < \infty, \tau X(x) < \tau\phi(i)\}$.

• $\{$the given packet is dropped due to channel error$\} = \{\tau\phi(i) < \infty, \tau\phi(i) < \tau X(x)\}$.

Based on our numerical studies using MATLAB, we plot some of our results into Figures 5.1 &5.2. In order to highlight some interesting characteristics of the EH-WSN node with temporal death, we present some observations in the following. Figs. 5.1 &5.2 give the death occurrence probability under different parameter λ, *ps*, *rw* and γSL. From Fig. 5.1(a) we can see when the arrival density λ decreases (the inter-arrival time of packets increases), the death occurrence probability decreases too. When the arrival density is small enough, the influence of the arrival density to the death occurrence becomes very weak. This fact is because that the decrease of the packet arrival density results in the decrease of the energy consumption of the communication, which then results in the decrease of the death occurrence probability. As expected, from Fig. 5.2(b) we can see that better the channel quality is, (*i.e.*, *ps* increases), smaller the death occurrence probability is. From Fig. 5.2(b), we can observe that when transmission rate from the sleeping to the listening γSL decreases, the death occurrence probability decreases, since the energy consumption decreases because of the increase of the sleeping time.



The death occurrence probability under different parameters:

Fig 5.1 (a) $\gamma-1$ *SL* = 50, $\gamma-1LS$ = 10, *ps* = 0.7 and *rw* = 0.25; (b) $\lambda-1$ = 1/10,$\gamma-1SL$ = 50, $\gamma-1LS$ = 10 and *rw* = 0.25.

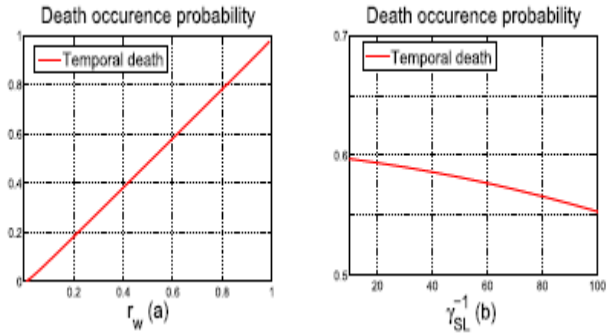


Fig 5.2 The death occurrence probability under different parameters:

(a) $\lambda-1$ = 1/10, $\gamma-1SL$ = 50, $\gamma-1LS$ = 10 and *ps* = 0.7; (b) $\lambda-1$ = 1/10,$\gamma-1LS$ = 10, *ps* = 0.7 and *rw* = 0.2

VI. CONCLUSION

The harvested energy is unable to provide a sustained energy supply to power the nodes in an EH-WSN continuously, the EH-WSN nodes can only be active for short periods of time, and the occurrence of temporal death in some nodes. The problem of secure provenance transmission in sensor networks, and identifies the challenges specific to this context, the secure provenance based encryption scheme and device a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes has been proposed. For future work, based on mathematical model and the metrices and optimization problem can be formulated to optimized the metrics of th EH-WSN by adjusting parameters.How to minimize the blocking and dropping

probabilities by adjusting the energy harvesting ability of the EH device in the sensor node, or by choosing the sleep and wakeup strategies under the QoS constraints would be interesting. Another question is to design an optimal routing protocol for the EH-WSNs that can be placed in the environment with poor energy resource to guarantee the QoS requirements.

REFERENCES

[1]. C. Alippi, G. Anastasi, M. D. Francesco, and M. Roveri, "Energy management in wireless sensor networks with energy-hungry sensors," IEEE Instrum. Meas. Mag., vol. 12, no. 2, pp. 16–23, Apr. 2009.

[2]. G. Anastasi, M. Conti, and M. Di Francesco, "Extending the life time of wireless sensor networks through adaptive sleep,"IEEE Trans. Ind.Informat., vol. 5, no. 3, pp. 351–365, Aug. 2009.

[3]. G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: A survey,"Ad Hoc Netw.,vol. 7, no. 3, pp. 537–568, May 2009.

[4]. S. Asmussen, "Matrix-analytic models and their analysis," Scandin. J. Statist., vol. 27, no. 2, pp. 193–226, Jun. 2000.

[5]. S. Asmussen, O. Nerman, and M. Olsson, "Fitting phase-type distributions via the EM algorithm,"Scandin. J. Statist., vol. 23, no. 4,pp. 419–441, Dec. 1996.

[6]. N. G. Bean and M. O'Reilly, "Performance measures of a multi-layer Markovian fluid model,"Ann. Operations Res., vol. 160, no. 1, pp. 99–120, Apr. 2008.

[7]. N. G. Bean, M. O'Reilly, and P. G. Taylor, "Hitting probabilities andhitting times for stochastic fluid flows,"Stochastic Processes Their Appl. vol. 115, no. 9, pp. 1530–1556, Sep. 2005.

[8]. A. Biason, and M. Zorzi, "Transmission policies for an energy harvesting device with a data queue," in Proc. IEEE Int. Conf. Comput., Netw. Commun. (ICNC),Garden Grove, CA, USA, Feb. 2015, pp. 189–195.

[9]. W.H.R.Chanet al., "Adaptive duty cycling in sensor networks with energy harvesting using continuous-time Markov chain and fluid models,"IEEE J. Sel. Areas Commun., vol. 33, no. 12, pp. 2687–2700, Dec. 2015.

[10]. C.-F. Chiasserini and M. Garetto, "An analytical model for wireless sensor networks with sleeping nodes," IEEE Trans. Mobile Comput. vol. 5, no. 12, pp. 1706–1718, Dec. 2006.