Detection of Replica Node Attack based on Exponential Moving Average Model in Wireless Sensor Networks

S.Anitha
Department of Information Technology
Kongu Engineering College
Erode, India
anithame@kongu.ac.in

P.Jayanthi
Department of CSE
Kongu Engineering College
Erode, India
jayanthime@kongu.ac.in

V.Chandrasekaran
Department of Medical Electronics
Vellalar College of Engineering and Technology
Erode, India
mail.vcresearch@gmail.com

***Abstract*—Owing to wireless communication's broadcast nature, Wireless Sensor Networks (WSNs) are vulnerable to several attacks. Amongst, replica attack is one of the predominant attacks as it facilitates the attackers to perform some other attacks. So, it is of great importance to design an efficient security scheme for WSNs. Since wireless sensor networks are energy restricted, introducing a trust method that assist the well-organized use of the available energy in each node is a primary design concern. In order to tradeoff between lifetime of the network and attack detection accuracy, energy based prediction approach is a suitable one. A statistical method, Exponential Moving Average (EMA) Model based replica detection (EMABRD) is proposed to detect replica node attack based on energy consumption threshold in WSNs. The difference between actual and predicted energy consumption exceeding the threshold level is considered as malicious one. The simulation results are taken using TRM simulator shows that choosing the threshold value neither too large nor too small produces optimum level of detection accuracy and lifetime of the network**

Keywords— WSN,exponential averaging, threshold, replica node.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are composed of a various number of scattered self-governing nodes whichcombinelymonitor physical or environmental features and send the data to a collecting node. It is widely used in numerous fields such as health-care, battle-field surveillance and environmental and habitat monitoring. Sensor nodes are deployed in distant and unattended places without equipped with tamper-resistant hardware. Because of wireless and distributed nature of WSNs, sensor nodes are risk to many attacks. The sensor nodes are inherent to various restrictions in terms of storage, computation and lifetime which make security solutions a big issue to implement in WSNs as specified in N. Alrajei et.al.,[5].

Though cluster-based WSNs are used to improve network lifetime, it is vulnerable to attacks as capturing the cluster head, the adversary can gain more information than a normal sensor node. As replica node paves way for other insider attacks like attack on routing, voting, fair resource allocation, data aggregation, distributed storage, and misbehavior detection, etc., it is important to defend against it. Replica attack is performed by creating multiple fake identities using existing one. Existing solutions are mostly based on key pre-distribution, node identities registration and position verification. Energy based prediction approaches are very few as indicated in Machaka et. al.,[8] and that too there is a gap between prediction accuracy and resource-constraint. In order to overcome this, prediction based on statistical method is proposed. Two features of EMABRD are listed as follows:

- EMABRD uses an exponential moving average model to predict nodes' energy consumption
- EMABRD detects replica node attack based on energy consumption thresholds

The content of this paper is organized as follows: Existing work of energy-based prediction in WSNs is introduced in Section 2. Assumptions about the network and threat models are given in Section 3. Replica attack detection method based on EMA is established in Section 4. The resilience of the proposed method is analyzed theoretically in Section 5. Simulation analysis and evaluation is provided in Section 6. Conclusion and future work is presented in Section 7.

II. RELATED WORKS

An Intrusion Detection System based Energy Prediction (IDSEP) for the cluster-based WSN was proposed by Han et al., [1]. Based on Markov chains, energy consumption prediction model is exploited for detecting the malicious nodes. Further, various categories of DoS attacks were determined based on the energy consumption thresholds. But it is not suitable for use it in real applications because of factors such as sensitivity, observation error, propagation delays, computation consumption, etc.,

Yu, Q., [2] proposed time series analysis which is useful in smart cities because many services generate time series data of which new observations are closely related to previous ones. For these types of data, static thresholds are not always adequate due to changing factors.

R. A. F. Mini., [3] adopted an energy prediction model. By knowing the nodes' states (sense, send, receive, sleep) from the past history and the amount of energy consumed in each state, energy dissipation rate is predicted. Based on which, generic prediction model is constructed to find energy consumption rate of each nodes and thus helps in detecting intruders in the network.

Energy map concept was introduced by F. Mini et. al.,[4] for predicting the lifetime of the network.Energy map is the energy remaining in each node of the network after every

operation. This concept is useful in many applications such as reconfiguration algorithms, query processing and data fusion. It is also used to deploy nodes in the low energy areas.

A security scheme named SSAD was proposed by Han et al., [6] for detecting DoS attacks in cluster-based WSNs. The method classifies nodes into three categories: trusted, un-trusted and uncertain that uses sole features to establish trustworthiness. Trustworthiness is assured by selecting cluster heads from the trusted domain. In the untrusted domain, untrusted nodes are removed and isolated from the network, while uncertain nodes join the clusters. These characteristics help to decrease the overhead involved in cluster head selection. In addition, it provides a competent solution to find and protectthe network against DoS attacks. However, cluster formulation is not explained in this paper. And also the SSAD approach is designed only for uniformnode networks but not useful for variednode networks.

Exponentially weighted moving average (EWMA) algorithm proposed by Opeyemi O., et. al., [7] uses received packet's inter-arrival rate to detect unevenalter in the strength of a jamming attack. The first phase is the training phase of capturing normal inter-arrival time from legitimate member nodes and cluster heads and given to the cluster head and base station respectively in order to initialize its parameters to obtain a normal profile. The second phase is the test phase in which pattern change is detected during jamming attack on a per packet basis using EWMA algorithm. Once the attack detection is done, an alarm is triggered and the malicious node isdetached from the network. The analysis shown in this paper includes only jamming attack detection with small or no overhead.

III. Markov Model Based Energy Prediction In Clustered Wsn

A. Energy dissipation model

A.1 Operational states of sensor devices

The operation modes of sensor nodes are modeled based on:

a. Combination of devices performing tasks such as monitoring, transmitting, receiving or processing

b. How sensor nodes monitor events occurring in the real environment considering factors sensitivity, observation error, propagation distance and communication and computation overheads

So, sensor nodes state transitions can be based on either event- or schedule-based one depending on the area they are deployed in for certain application.

In event-based, sensor nodes continuously sense their devices for the occurrence of a random event. True event value is determined based on the threshold set for parameter value to be sensed.

In schedule-based, sensor nodes sample the sensor device following a predetermined time schedule for monitoring temperature, humidity, pressure, water level, gas leakage etc.,

The combination of different operational modes of sensor devices like processor, memory, sense and radio unit contributes to the different states of the sensor device. The operational state of different components of sensor node is shown in Table I.

TABLE I. COMPONENTS OPERATIONAL MODES IN DIFFERENT STATES

States of sensor node	**Processor**	**Memory**	**Sensor device (Sense unit)**	**Transceiver (Radio unit)**
Calculating	Active	Active	Off	Receive and Transmit
Transmitting	Active	Active	Off	Transmit
Sensing	Sleep	Sleep	On	Off
Receiving	Active	Active	Off	Receive
Listening (Monitoring)	Idle	Sleep	On	Receive
Sleeping	Sleep	Sleep	Off	Off

Some other combinations of operation modes are not considered as states due to their unimportance in power saving or unrealistic operational mode. For instance, memory does not be in sleep mode when the processor is in active so it will not contribute in power saving.

A. Energy Prediction

In Han et al., [1], prediction model based on probability was proposed, in which sensor nodes operation modes are represented by the states of a Markov chain. Sensor node's each state entry probability is denoted by a random variable. The sensor node shifts its state based on the operation of sending or receiving the packets or calculating the value or sensing the data. It is assumed that each sensor has L modes of operations, so each node is modeled by a Markov chain with L states. Energy dissipation mainly focuses on sensing, transmitting, receiving and calculating, so with these four states each sensor node is modeled by a Markov chain.

Onetime step is defined as the smallest amountof time unit of the four operation states with each state covering several time steps. If a node is currently in state i, then the probability of the node transiting to state j in next(one) time-step is represented by p_{ij} for $i, j = 1,2,3,4$. The node taking n transitions (time steps), the operation states can be denoted as $X = \{X_0, X_1, \ldots, X_n\}$ with transition probability $P_{ij}^{(n)}$ in moving from state i to state j can be formulated as:

$$P_{ij}^{(n)} = P\{X_{n+m} = j \mid X_m = i\} \quad (1)$$

Using Chapman-Kolmogorov equation,

$$P_{ij}^{(n)} = \sum_{k=1}^{m} P_{ik}^{(r)} P_{kj}^{(n-r)} \; where \; 0 < r < n \quad (2)$$

If the monitoring node knows $P_{ij}^{(n)}$ and initial states of the monitored nodes, then energy dissipation information can be predicted for all the nodes in the network.

The three steps in the prediction process are:

- With p_{ij}, it is possible to predict a node's amount of time steps in moving from initial state x_0 and stays in state j, in the next T time steps $\sum_{t=1}^{T} P_{ij}^{(t)}$.
- The monitoring node calculates the amount of energy dissipated in the next T time steps, E^T is given by,

$$E^T = \sum_{j=1}^{L}(\sum_{t=1}^{T} P_{ij}^{(t)}) * E_j \quad (3)$$

where E_j = energy dissipated by a node in state j for one time step.

1. The monitoring node calculates the energy dissipation rate (ΔE) of the monitored nodes in next T time steps. By decreasing the value ΔE periodically from the amount of residual energy of each node, monitoring node can maintain energy dissipation estimations in each monitored node. The cluster head send the predicted dissipated energy to the base station where trust information is stored.

The drawback of the Markov model for energy prediction is that it requires lot of computation as each node has to follow its current state at each time-step. For this, probability matrix has to be maintained by each node updating its state at each time-step.

IV. Network Model

A. Assumptions about the network

The following assumptions are made about the network:

- Nodes are static, uniformly deployed and equipped with omni-directional antenna
- Homogenous network using greedy routing protocol
- Sensor nodes in the same state (transmit/receive/sense/calculate/sleep) consume same amount of energy at any period of time and

B. Assumptions about the attacker

The following assumptions are made about an attacker:

- Attacker can create as many replica of the captured sensor node and
- Attacker can modify the energy value of the captured node

V. EMA model based energy prediction for replica node detection scheme in clustered WSN

The proposed method can be divided into three steps viz., energy prediction model, threshold setting and replica node detection process that works based on the event (periodic or random)

A. EMA model for Energy prediction

Let us take a sensor node has Koperation modes. The duration that the node spends in each state should be forecasted with a guaranteed accuracy in order to predict the amount of energy the node will dissipate in the next T time-steps. Let ΔE represents the amount of energy consumed by a node in a period of time Tand let Δe represents the amount of energy dissipated by the node in a single state. Mathematically, relationship between Δe and ΔE can be represented as:

$$\Delta E = \sum_{i=1}^{k} \Delta e_i \quad (4)$$

From above equation (4), it can be seen that the amount of energy consumed in each state on which total amount of energy spent by a node in certain period of time depends. Using the following equation, energy consumption in each state, Δe can be calculated as,

$$\Delta e_i = Q_i * t_i \quad (5)$$

where Q_i is a constant which represents energy spent per unit time in state i and t_i represents the duration of time a node spent in state i. During each time period T, the dissipated energy in each state is directly proportional to the length of time t the node stayed in that state. From equations (4) and (5), effective prediction is made by accurately predicting the length of time a node spent in each state. Using accumulative average of the measured length of the previous times the node spent in each state, the length of the duration a sensor node spends in a certain period can be predicted. The exponential average prediction formula is given below:

$$I_{n+1} = ai_n + (1-a)I_n \quad (6)$$

where I_{n+1} is the next predicted period length a node stays in state i,

I_n is the previously predicted period,

i_n is the recent time period the node actually spent in state i

a is a attenuation factor which is constant lies in the range (0,1)

When $a = 1$, the next predicted period will depend only on actual period i_n. When $a = 0$, the future time period the node spends in state i will be predicted based on only the last predicted period. Equation (6) can be further expanded as

$$I_{n+1} = ai_n + a(1-a)i_{n-1} + \cdots a(1-a)^n i_0 + a(1-a)^{n+1} I_0 \quad (7)$$

Equation (7) shows that the predicted period is the weighted average of previous periods the node was in state i. It can be used to predict the next length of time a node spends in each state i. Let x represent the time t_i, a node spends in state i and X represents the predicted duration a node will spend in state i. Rewriting equation 7,

$$X_{n+1} = ax_n + a(1-a)x_{n-1} + \cdots a(1-a)^n x_0 + a(1-a)^{n+1} X_0 \quad (8)$$

Extreme case:

Sometimes a node unexpectedly might stay in one state than the usual routine. In that case, equation (8) cannot be effective. After similar length of periods, occurrence of unexpected long period will affect the result of next prediction. If the upcoming predicted period X_{n+1} , is greater than the previous predicted period X_n multiplied by a threshold c, where c is greater than one, then the next predicted value will be multiplied with the previous predicted value and the threshold in order to minimize the error caused by overestimation. It is shown in equation (9) as,

$$if(ax_n + (1-a)x_n) > cx_n X_{n+1} = cX_n \quad (9)$$

B. Threshold setting

When setting threshold based on the prediction error P_{error} , total energy spent in different states E and total messages sent and received count isN_{sr} was considered.The tradeoff between detection accuracy and energy consumption can be measured with varying levels of threshold with the prediction period. It can be defined as shown in equation (10).

$$\mathrm{Th} = \frac{\mathrm{P_{error}}}{\mathrm{E+N_{sr}}} * 100 \quad (10)$$

where

$$\mathrm{P_{error}} = (\mathrm{ap} - \mathrm{at}) * 74.7 + (\mathrm{lp} - \mathrm{lt}) * 52.2 + (\mathrm{sp} - \mathrm{st}) * 38.72 + (\mathrm{slp} - \mathrm{slt}) * 0.0285 + \mathrm{N_{error}}$$

$$\mathrm{E} = \mathrm{at} * 74.7 + \mathrm{lt} * 52.2 + \mathrm{st} * 38.72 + \mathrm{slt} * 0.0285$$

$$\mathrm{N_{sr}} = (50\mathrm{e} - 4 * 500 + 100\mathrm{e} - 4 * 400 * 500) * \mathrm{c\_nms} + 50\mathrm{e} - 4 * 500 * \mathrm{c\_nmr}$$

$$\mathrm{N_{error}} = (50\mathrm{e} - 4 * 500 + 100\mathrm{e} - 4 * 400 * 500) * (\mathrm{p\_pred\_nms} - \mathrm{c\_nms}) + 50\mathrm{e} - 4 * 500 * (\mathrm{p\_pred\_nmr} - \mathrm{c\_nmr})$$

The variables meaning are given in Table II

TABLE II. ABBREVIATIONS AND ITS MEANING

Symbols	Meaning
Th	Threshold
P_{error}	Prediction error (difference between actual and predicted energy in different states)
E	Total energy spent in different states
N_{sr}	Total number of messages sent and received
N_{error}	Difference between the predicted and actual number of messages sent and received
ap	Active period
at	Active time
lp	Listen period
lt	Listen time
sp	Sense period
st	Sense time
slp	Sleep period
slt	Sleep time
c_nms	Actual number of messages sent
c_nmr	Actual number of messages received
p_pred_nms	Predicted number of messages sent
p_pred_nmr	Predicted number of messages received

C. Detection of replica node

The comparison between the energy prediction result and the real energy consumption was made to detect malicious node by using EMA method. To launch replica attack, additional energy was spent by malicious nodes. Therefore, if there is significant difference between the energy prediction results and real energy consumption of nodes, multiple identities of malicious nodes (replica nodes) can be detected. Let T_x' and T_x denote the predicted and real energy consumption respectively. The proposed method detects the replica node when the following condition is satisfied as given in equation (11),

$$\frac{T_x'}{T_x} > th \quad (11)$$

VI. THEORETICAL ANALYSIS

Node ihas virtually multiple identities in a replica attack. Assuming m_i is the number of identities among which only one identity is real, other $m_i - 1$ identities are fake. So, node i can pretend as any ofm_i nodes. Therefore replica nodes consumes $m_i T_x$ amount of energy i.e., m_i times as much energy as the normal one. Then the predicted expenditure of energy is T_x' and ρ be the size of the network.

$$\frac{T_x'}{T_x} < th \Rightarrow \frac{T_x'}{m_i T_x} < \frac{\rho T_x'}{(\rho-1)T_x}\frac{1}{m_i} < \frac{\rho}{(\rho-1)} \Rightarrow m_i > 1 - \frac{1}{\rho} \quad (12)$$

Thus the EMA scheme detects replica attack of node iwhen$m_i \leq 1 - \frac{1}{\rho}$

VII. SIMULATION ANALYSIS

A. Simulation setup and operation

In EMABRD, all sensor nodes are assumed to be static and with inadequate energy level in the batteries. Replacement of depleted batteries is considered as impossible. All the sensor nodes are deployed randomly with only one sink node. The sink node is assumed to have enough energy for staying alive until the last node dies and is centered. In the simulation, all the sensor nodes are assumed to know about their geographical location for the greedy forwarding routing of packets. The simulation parameters are specified in Table III.

TABLE III. SIMULATION SETUP

Parameters	Values
Node deployment	Random
Transmission range	15m
Bandwidth of channel	1 Mbps
Time of simulation	500 s
Mode of propagation	Free space
Size of packet	512 bytes
Number of nodes	100
Initial energy	200J
Area of deployment	100m X 100m
Sink Node Position	x=50m, y=50m

In the simulation, each node while residing in different states for several time-steps periodically calculates the amount of energy it consumed. The monitoring node predicts the amount of energy the node will consume in next several timesteps. If the difference between the actual energy consumption and predicted energy consumption exceeds the defined threshold, then that node is considered as replica. Assuming the events are periodic, all the sensor nodes send their residual energy and energy consumption rate periodically to the monitoring node.

In order to measure the performance of the proposed method, the network is implemented with 100 nodes. Nodes in the network use a greedy routing protocol called most forward within radius (MFR), to route packets to the sink node. A node S using MFR routes data to a node E in its coverage, nearest to the sink when projected to a line connecting the sender node S and the sink D. Sensor nodes use location advertisement message to notify their location to their neighbors through routing table and choose the nearest next hop for forwarding data to the sink.

B. Simulation results

The proposed method is implemented using TRM simulator. The first section analyzes the difference between residual energy in each nodes and the value registered in the monitoring node for different value of threshold. In the last section, the relation between the number of energy packets sent to the monitoring node and the threshold value used is discussed.

- *Energy cost*

The average number of messages sent to the monitoring node is higher for all threshold values using exponential average model over markov chain model in case of uniformly distributed events. But, in case of periodic events, the average number of messages sent to the monitoring node is lesser for all threshold values using exponential average model over markov chain model.

This is due to the reason that exponential averaging method predicts the upcoming energy consumption of the nodes based on their energy consumption history. Due to the arrival of unexpected events, some of the nodes energy consumption behavior might deviate from the average energy they were using in the past. This influences the nodes future energy depletion predictions, prompting the nodes to send higher number of packets.

For uniformly distributed event arrival model, the maximum number of energy packets sent per node reaches up to fifteen for the model used in this work, when the threshold is set to 1%, whereas, for probabilistic model, the maximum remains at an average of nine energy packets per node for the same threshold. When the number of energy packet sent to the monitoring nodeis increased, energy cost increases.

In case of strictly periodic event arrival model, EMA model shows better performance compared to the Markov model [4] when the threshold is set to 1% and 3%. The maximum number of energy packets sent per node in EMA model is around six packets, at a threshold of 1%, which is less than the number of energy packets sent by the Markov model [4]. This is because of the constant energy consumption behavior of nodes related to the periodic nature of event occurrences. These reductions in the number of energy packets sent, directly contribute to the minimization of energy cost.

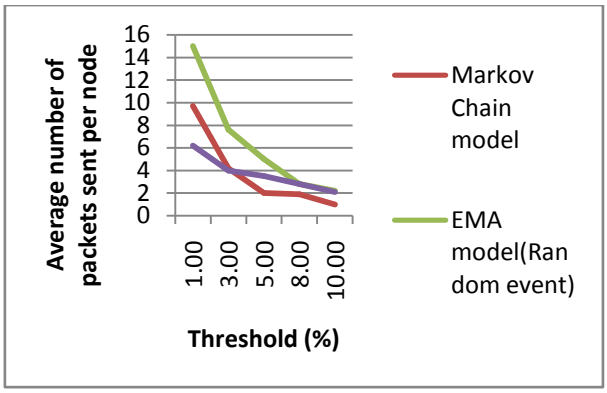

Fig.1. Average number of packets sent per node over various threshold values

- Energy Monitoring Error

Energy monitoring error is the difference between the remaining energy in individual node and the remaining energy of each node registered in the monitoring node. Fig. 2 shows the deviation between real energy remaining in each node and the values registered in the monitoring nodes for the nodes in the network which increases as the value of threshold is increased.

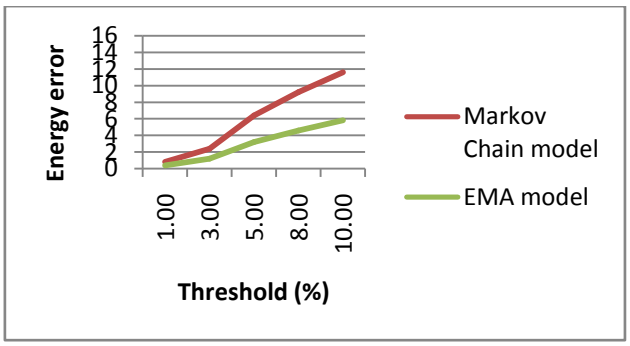

Fig.2. Energy error over various threshold values for the prediction period$T = 300s$ when the event is strictly periodic

Due to the reason that nodes do not send energy packet to the monitoring node unless the difference between the real energy consumption and the predicted energy depletion is greater than the threshold value set. As a result, prediction errors less than the threshold are accumulated in the monitoring node creating greater deviation for higher threshold values. The figures demonstrated that when higher threshold values used the energy deviation increases, reaching up to 12J when the threshold is set to 10%. When a threshold of 1 percent is used, the energy deviation has reached its minimum, 0.1J. Although threshold reduction has the advantage of reducing the energy information deviation between the residual energy in the sensor nodes and the monitoring node but increases the number of energy packets sent to the monitoring node.

- Detection rate

In Fig. 3, detection rate of Exponential Moving Average model is nearly 1% higher than the Markov chain model for different values of threshold is shown. The higher detection ratio lies in the fact that malicious nodes have to spend additional energy than that of normal nodes to conduct replica attack. Using this characteristic, EMA model efficiently detects attack nodes based on energy consumption rate. Threshold value is calculated by considering propagation delay of messages received from each sensor nodes in addition with past conversation history.

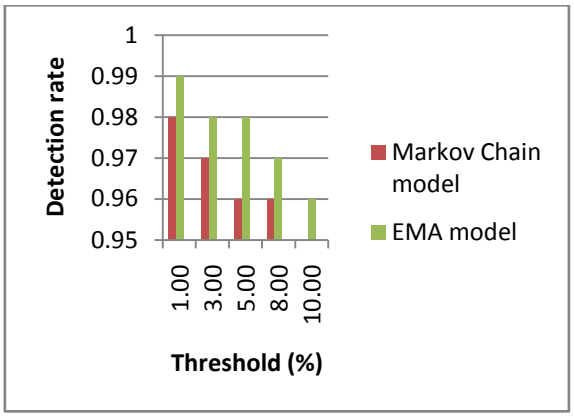

Fig.3. Detection rate for different threshold values when the event is random

As shown in Fig. 4, the number of survival nodes decrease sharply for increasing number of rounds in the simulation. The survival rate is slightly higher in EMA model compared to Markov Chain model due to infrequent transmission of packets between the sensor nodes and monitoring node.

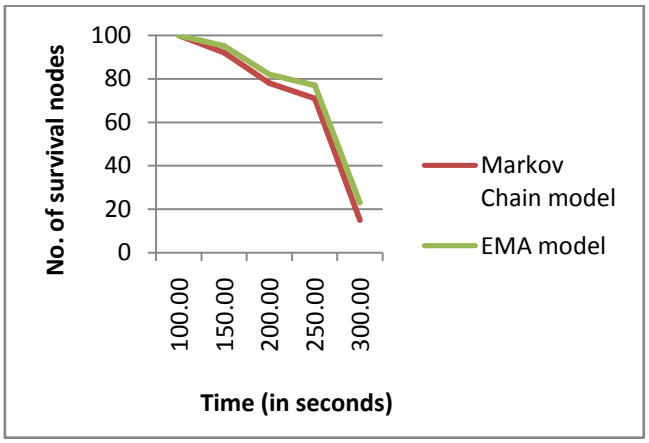

Fig.4. Number of survival nodes in different time periods of simulation

VIII. Conclusion and Future Work

In this work, Exponential Moving Average Model is presented to build the residual energy and replica node detection based on threshold value. It is also used to predict the upcoming energy consumption in each node based on the previous power depletion history of the node. Each node forwards the predictable power consumption rate and its available energy to the monitoring node. Nodes send an update to the monitoring node only if the difference between previously predicted consumption rate and the actual energy depletion rate is higher than the threshold set.

The simulations conducted showed that in prediction-based approach using exponential moving average algorithm, the number of messages sent is less than in F. Mini et.al., [4] by 30% when the threshold is set to one percent and arrival of events is assumed to be periodic. This is due to the reason that exponential moving average algorithm makes use of previous history of energy consumption to predict future consumption.As a result, it adapts to changes in the environment such as frequent occurrence of events. The simulation results have also shown that the error between the residual energy information recorded in the monitoring node and the actual residual energy in each node is minimized when the threshold is set closer to zero, but the energy cost of monitoring residual energy distribution has increased sharply. Therefore, a tradeoff has to be made between the accuracy of the residual energy information in the monitoring node in order to detect replica node and the amount of energy spent. Solar energy prediction algorithm [Sharma et. al., 9, Z. Jiang et. al.,10] in real working environment will be experimented in future.

References

[1] G Han, J Jiang, W Shen, et al. “IDSEP: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks”, IET Information Security, Vol. 7, Issue 2, 2013, pp. 97-105

[2] Yu, Q.; Jibin, L.; Jiang, L., “An Improved ARIMA-Based Traffic Anomaly Detection Algorithm for Wireless Sensor Networks”, Int. J. Distrib. Sens. Netw, 2016

[3] R. A. F. Mini, B. Nath, and A. A. F. Loureiro, “A probabilistic approach to predict the energy consumption in wireless sensor network”, in IV Workshop on Wireless Communication and Mobile Computing, 2002

[4] F. Mini, M. do Val Machado, A. Alfredo F. Loureiro, and B Nath, “Prediction-based energy map for wireless sensor networks, AdHoc Networks”, Vol.3, Issue 2, 2005, pp.235-253

[5] Nancy Alrajei, George Corser, Huirong Fu and Ye Zhu, “Energy Prediction Based Intrusion Detection in Wireless Sensor Networks”, International Journal of Emerging Technology and Advanced Engineering, Vol. 4, Issue 2, 2014

[6] Han, G., Shen, W., Duong, T. Q., et al., “A proposed security scheme against Denial of Service attacks in cluster-based wireless sensor networks”, Security Communication Networks, Vol. 7, 2014, pp. 2542–2554

[7] Opeyemi O., et. al.,“A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks”, sensors, Vol. 18, Issue 1691, pp. 1-15

[8] P.Machaka, A.Bagula, F.Nelwamondo, “Using Exponentially Weighted Moving AverageAlgorithm to Defend Against DDoS Attacks”, Pattern Recognition Association of South Africa and Robotics and Mechatronics, International Conference (PRASA-RobMech), IEEE, 2016

[9] Himanshu Sharma, Ahteshamul Haqueand Zainul A. Jaffery, “Solar energy harvesting wireless sensor network nodes: A survey”, Journal of Renewable and Sustainable Energy, vol.10, issue 2, 2018

[10] Z. Jiang, X. Jin, and Y. Zhang, “A weather-condition prediction algorithm for solar-powered wireless sensor nodes”, IEEE 6th International Conference on Wireless Communications, Networking and Mobile Computing, 2010

[11] Jie Wu and Shuhui Yang, ”Energy Efficient Node Scheduling Models In Sensor Networks With Adjustable Ranges”, Special Issue: Advances in Parallel and Distributed Computational Models, International Journal of Foundations of Computer Science, Vol. 16, No. 01, pp. 3-17, 2005

[12] Mitali Singh and Viktor K. Prasanna,“Hierarchical model for distributed collaborative in Wireless Sensor Networks”, International

Journal of Foundations of Computer Science, Vol. 22, No. 04, pp. 983-998, 2011

[13] Debashis Mondalet.al.,"Measuring the quality of surveillance in a Wireless Sensor Network", International Journal of Foundations of Computer Science, Vol. 15, No. 03, pp. 485-506, 2004