Resourceful Adaptive Encapsulation Based Logo Pattern Matching Algorithm for Intrusion Detection In Wireless Sensor Network

R. Hamsaveni[1], Dr. G. Gunasekaran, M.E., PH.D[2] (Engg)

[1]*Research Scholar, SCSVMV University, Kanchipuram*

[2]*Principal, Meenakshi College of Engineering, Chennai*

Abstract: Wireless Sensor Networks (WSNs) have been gaining interest as a platform that change on the basis of interaction with the physical world. Security is important for many sensor network applications. Intrusion Detection Systems (IDS) are helpful in detecting those attacks, but they are computationally expensive and require enormous resources for detecting the threats. The proposed method is a novel methodology to detect wormhole attack in network and power consumption to detect this attack is greatly reduced is proven. The main objective is to develop a simple Resourceful Adaptive Encapsulation based Logo Pattern Matching algorithm (RAELPM) for detect and isolate wormhole attack in the network and increase the throughput of the network. As sensor nodes are battery-powered devices, the critical aspect is to reduce the energy consumption of nodes, so that the network lifetime can be extended to reasonable times. So, attempts are made to design and develop algorithms that are energy efficient supporting the IDS of WSN. The proposed algorithm considers three stages they are, Neighbor Identification and List Creation, Suspicious Set Creation and Detection Based on RAELPM. A Neighbor Identification and List Creation is used to Base Station (BS) is the central node that is fixed in a communication range. Suspicious Set Creation Each sensor node has a counter along with it. The counter of each node is monitored by the Base Station. The counter value is initialized to 0 before getting processed. Each node gives or gets data, and when that happens, the value of the counter gets incremented automatically when it processes data. Then finally, Base Station monitors each node included in the suspicious set. BS sends a hello request to both suspicious node and its neighbors in the neighbor list. If the node along with its neighbors replies to the Base station, then that node is not a wormhole and is considered to be genuine. The proposed work gains low cost, low energy for sensor nodes compared to other techniques used in existing methods.

1. Introduction:

Majority of networks, like a peer-to-peer network, depend on suppositions of identity, where each system characterizes a single identity. Troubles occur when a reputation system is deceived into believing that an attacker has a disproportionally large authority. Likewise, an attacker with multiple identities can utilize them to operate maliciously, by either embezzling data or disrupting communication between nodes. Such an attack is an attack that threatens the reputation system of a peer-to-peer network by launching a huge number of pseudonymous identities, utilizing them to acquire a disproportionately large authority.

Thus, in the attack, by imitating other nodes in the network or merely by claiming fake identities, a malicious node conducts itself as if it were a larger number of nodes. A Sybil attacker may also create a random number of supplementary node identities, using only a single physical device.

A reputation system's weakness to a Sybil attack relies on how cheaply identities can be engendered, the level to which the system of reputation agrees inputs from node entities that lack a chain of mutual trust connecting them to a trusted entity, and if the system of reputation cares for all entities identically. A section of software that has access to local resources is known as an *entity* on a peer-to-peer network. The objective of an entity is to advertise itself on the network by offering an *identity*. Multiple identities can relate to a single entity.

Otherwise said the mapping of identities to entities is many to one. The purposes of entities using multiple identities are for redundancy, resource sharing, reliability, and integrity. In peer-to-peer networks utilization of the identity is in the form abstraction thus a remote entity becoming conscious of identities without essentially knowing the association of identities to local entities. By default, each unique identifier is normally assumed to correspond to a unique local entity. In reality, multiple identities may get associated to the same local entity.

One of the ways to launch the attack is by having nodes communicating directly with positive nodes. When a valid node transmits a message to a node, one of the malicious devices hears the message.

Similarly, messages sent from nodes are in reality transmitted from one of the malicious devices. When no positive node can communicate directly with the nodes, it is said to be in indirect communication. Instead, more than one of the malicious nodes declare that they can reach the nodes. Routing is performed via one of these malicious nodes when messages are transmitted to a node.

From Figure 1.1, it is appreciated that faulty node or an adversary may exhibit different identities to a peer-to-peer network to seem and function as multiple distinctive nodes.

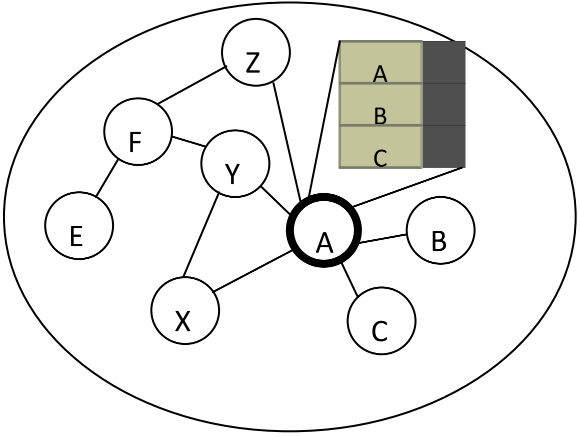


Figure1.1 Scenario of Sybil node

After becoming a part of the peer-to-peer network, the attacker might then eavesdrop on communications or perform maliciously. By masquerading and exhibiting several identities, the attacker can take charge and influence the system significantly.

Another likelihood is that the adversary could possess quite a few physical devices in the network, and might have these devices change over identities. While the number of identities the attacker exploits and a number of physical devices are the same, each device exhibits different identities at distinct times.

2. Related Works:

There are few works done before which motivated us to devise our mechanism. In this section, we note those briefly. The vulnerabilities of the trust mechanism are addressed in [1-2]where the authors discuss the various weaknesses of the stages of trust mechanism.

The idea is to compare the signal strength from the reception side with its expected value. A signal is only detected by a receiving node if the received signal power is equal or greater than the received signal power threshold [2-3]. If the signal power received is less than the threshold, then the particular node is suspected to be malicious. This may not be true for all cases. A signal power can be weakened due to various reasons like environmental factors, obstacles, genuine power shortage, etc.

In this mechanism, the sending node stores all recently sent packets in its buffer and compare each packet with the overheard packet to see whether there is a match. If positive, it means that the packet is forwarded by the neighboring node and the sender would remove the packet from the buffer [4-5]. This methodology’s drawback is that it requires sniffing enough number of data packets to decide whether a node is an attacker. This means that more time is needed to make a decision compared to a network without a tolerance threshold. If the attacker is moving, there is a possibility that the malicious node moves outside the detection signal range and thus, it could not be detected.

Several works that used neighbor-based approach are introduced to mitigate selective forwarding attacks. The work used a monitoring neighbor that warns the sending node and the Base Station (BS) when insider attacks by dropping packets [6-7]. The limitation of this method is understood when neighbor nodes falsely accuse good nodes as attackers.

Here, relative communication overhead regarding a number of compromised nodes seems to be higher. The algorithm for detection, diagnosis, and isolation of nodes launching control attacks such as Wormhole, Sybil, Rushing, Sinkhole and Replay attacks [8]. But, the limitation of the methodology lies in its difficulty when used for mobile networks.

The authors have proposed a methodology for monitoring the neighbor by virtually extending the nodes’ monitoring coverage [9-10]. The disadvantage of this method is that the selective packet drops are not addressed.

An improved detection monitoring system has been developed based on a power-aware hierarchical model [11-12]. The methodology resolves the ambiguous Collision.

The authors have proposed an energy model that includes the various sources of energy consumption like transmitting energy, sensor sensing, sensor logging, and actuation [13-14]. They have included other sources of energy consumption which other models have not dealt with. The authors have discussed the impact of overhearing transmissions on total energy costs during data gathering and dissemination [15-16]. They have incorporated overhearing cost into the energy equation that suits well for calculating the energy consumption using the proposed technique.

The introduced a comprehensive node energy model, which includes power components for radio switching, transmission, reception, listening, and sleeping. Some works have also gone into the direction of Sybil attacks that have assisted in bringing out a solution for the same if the Sybil node replies with same identity and different locations [18-19]. The existing mechanisms for detecting Sybil attacks include both centralized and decentralized approaches.

In this case, the authors propose a particular trusted third party or central authority, which can verify the validity of each participant. It issues a certification for the honest one [20]. In reality, such certification can be a special hardware device or a digital number. Note that essentially both of them are a series of digits, but are stored on different media.

Before a participant joins a peer-to-peer system, provides votes, or obtains services from the system; first, his identity must be verified [21-22]. This method shows its limitation when it is applied to the larger network. If a Sybil node exists, then it has to perform the tasks of the identities it possesses.

Consequently, when it exceeds a threshold value, the Sybil node is detected. In Though it is said to be lightweight, it is time-varying, unreliable and radio transmission is non-isotropic [23-24]. Accuracy reduces as the transmission distance increases. Recent works on Sybil defense mechanisms are based on Social network based schemes.

3. Materials and Methods:

From the literature review, it is understood that an algorithm is required to detect node as well as to conserve energy during the process. While many other wireless networks may successfully use many existing solutions, for WSN, this is imperative to save energy alongside the efficiency of the mechanism. With this motivation, we propose here a novel algorithm. A major challenge in constructing a WSN is to enhance the network lifetime. Nodes in a WSN are usually highly energy-constrained and expected to operate for longer periods. Accurate prediction of sensor network lifetime requires an accurate energy consumption model. In this work, a comprehensive energy model is adopted that includes sensing, logging and switching energies apart from the processing and communication energy values.

The proposed work of detecting the IDs is done using 3 phases. They are:

A) Neighbor Identification and List Creation
B) Suspicious Set Creation
C) Detection Based on RAELPM

3.1 Neighbor Identification & List Creation

In the proposed method, the Base Station (BS) is the central node that is fixed in a communication range. BS sends a route request to all the nodes present in the network. After sending a request message, the BS expects a reply from all the nodes to become neighbors to the BS. The nodes that reply are accepted inside the network. The Base station saves each node's ID. The nodes which have not responded are considered to be out of the network. After the route is created between individual nodes to their neighbor nodes the distance between them is calculated. The nodes that are saved in BS is now determined by its co-ordinates by a basic mathematical equation. Let ‘D’ be the distance between any two nodes with coordinates (x1, y1) and (x2, y2). The distance between two the nodes is calculated by Euclidean distance method given by equation (3.1).

$$D = \sqrt{(y_2 - y_1)^2 + (x_2 - x_1)^2} \qquad \ldots 3.1$$

The Neighbor list is created and saved in Base station for each and every node in the network.

Table 3.1 summarizes the major mathematical notations used in this work.

Table 3.1 Major mathematical notations used

Notation	**Meaning**
^{E}loggn	Energy consumption for sensor logging
^{E}write	Energy consumption for writing data
^{E}read	Energy consumption for reading data
b	Number of bits in a packet
^{V}sup	Supply voltage to sensor
^{I}write	Current for writing 1-byte data.
^{T}write	Time duration for flash writing
^{I} read	Current for reading 1-byte data
^{T}read	Time period for flash reading
^{E}txn	Energy dissipation due to transmit of b bit packet
^{E}elec	Energy dissipation: electronics
n	Distance-based path loss exponent
^{d}ij	Distance between sensor Nodes
amp	Energy dissipation: power amplifier
^{E}rxn	Energy dissipation due to Receiving *b* bit packet
^{E} switch	Energy consumed for switching the radio from sleep mode to active mode
^{I}active	Current draw of the radio in active mode
I	Current draw of the radio in sleep mode
T	Time required for the communication to go from sleep mode to active mode
^{E}ij	Total energy expenditure due to a transmission from node to

$N_{ij}oj$	Some nodes within the communicating radius of i when it communicates with j.
^{E} total	Total energy consumed by each and every node
mcu	Energy consumed due to processing of packets
I_0	Leakage current
h1	Weighting factor: Processing
h_2	Weighting factor :Transmission
h_3	Weighting factor :Receiving
h_4	Weighting factor :Sensing and sensor logging
N_{cyc}	Number of clock cycles per task
C_{avg}	Average capacitance switch per cycle
f	Sensor frequency
n_p	Constant: Processor dependent
Eactu	Energy dissipation: actuation

3.2 Suspicious Set Creation:

Each sensor node has a counter along with it. The counter of each node is monitored by the Base Station. The counter value is initialized to 0 before getting processed. Each node gives or gets data and when that happens, the value of the counter gets incremented automatically when it processes data. A maximum threshold is set for the counter. Here the threshold value is set to 25. When the traffic in each sensor exceeds the counter value of 25, the maximum limit, the Base Station includes the node in the suspicious set. Similar procedure is adopted for all the nodes in the network and if the traffic is more in those nodes they are also put under suspicious set. The sink of the WSN receives the packets when the nodes respond to it in the routing path. It then analyses for the malicious nodes. Let it be assumed that a node returns with ‘1' as its status bit for a negative packet and ‘0' for a positive packet. The node that does not respond has a status bit value, ‘-1'. A suspicious set is generated that contains nodes having status bit ‘-1'. These nodes are not straightly marked as malicious nodes since the packets from the nodes may not have been received by the sink due to interference or poor communication quality.

Sensor logging consumes energy used for reading ‘*b*’ bit packet data and writing it into memory. Sensor logging energy consumption for a node per round is evaluated.

$$E_{loggn}(b)=E_{write}+E_{read}=\frac{b\times V_{sup}(I_{write}\ T_{write}+I_{read}\ T_{read})}{8}$$

..3.2

Where Ewrite is energy consumption for writing data, Eread is energyconsumption for reading ‘*b*’ bit packet data, I write, and I read are current forwriting and reading 1-byte data.Communication of neighboring sensor nodes is enabled by a sensornode. Energy dissipation by a sensor node can be attributed to transmitting andreceiving data. The energydissipation due to sending ‘*b*’ bit packet, in a distance dij from the sensor nodeto the neighbor.

$$E_{txn}\left(b,d_{ij}\right)=b\times E_{elec}+bd_{ij}^{n}\times E_{amp}\qquad\text{…3.3}$$

Where Eelec is the energy dissipated to send or receive electronics, Eamp isthe energy dissipated by the energy and is the distance-basedpath-loss exponent. Here, free space spading is assumed and so _ takes thevalue.

Energy dissipation due to receiving ‘b’ bit packet from the sensor node is given by:

$$E_{rxn}(b)=b\times E_{elec}\qquad\text{… 3.4}$$

The switching energy component is the energy consumed for switching the radio state between states, including normal, power down and idle modes. The following equation determines the energy consumed for switching the radio from sleep mode to active mode. In the energy model that incorporatesoverhearing, the total energy expenditure due to a transmission from node to is given by,

$$E_{ij}\left(b,d_{ij}\right)=b\times E_{elec}+bd_{ij}^{n}\times E_{amp}+N_{ij}^{(oj)}\times E_{rxn}(b)\qquad\text{…3.5}$$

Hence, the total energy consumed by a node is given by,

$$E_{total}=E_{mcu}+E_{switch}+E_{txn}+E_{rxn}+E_{loggn}\qquad\text{… 3.6}$$

Etotalis the total energy consumed by every node, Emcu is the energy consumed due to the processing of packets, Eswitch is the switching energy.The total energy consumed by the Cluster, CHj per round is given byequation

$$E_{CH}(j)=E_1+E_2+E_3+E_4+E_5+E_6+E_7\qquad\text{…3.7}$$

Where

$$E_1=h_3\times b\times V_{sup}\times I_{sense}\times T_{sense}\qquad\text{…3.8}$$

Stands for energy due to sensing

$$E_2=h_4\times b\times V_{sup}(I_{write}\times T_{write}+I_{read}\times T_{read})\qquad\text{…3.9}$$

Is the data logging energy,

$$E_3=h_1\times b_1\times N_{cyc}\times C_{avg}\times V_{sup}^{2}\left(n_j+1\right)\qquad\text{…3.10}$$

Is the energy spent due to switching,

$$E_4=h_1\times b_1\times V_{sup}\left(I_0\times e^{(V_{sup}/N_pVT)}\right)\left({}^{N_{cyc}}/_{f}\right)(n_j+1)\qquad\text{…3.11}$$

Stands for the leakage energy,

$$E_5=h_2\times b_2\times(1+\gamma)\times d_j^{n}\times E_{amp}\qquad\text{…3.12}$$

Is the transmiting energy consumed by the nodes ti the CH,

$$E_6=T_{CH}\times V_{sup}[C_{CH}\times I_A+(1-C_{CH})I_S]\qquad\text{… 3.13}$$

Is the energy spent during transient,

$$E_7=E_{actu}\times N_{actu}\qquad\text{… 3.14}$$

Is the actuation energy.

Algorithm:

Let the WSN has a collection of sensor nodes

The source sends data packets to nodes

1. **for** each intermediate node on a routing path from the Source to Sink
2. Sink verifies their sequential numbers
3. **if** Sink detects a discontinuous sequential number
4. Sink broadcasts an alert packet
5. **end if**
6. **for** each intermediate node receiving the alert

```
it checks the packets within its cache
if it detects a missing packet
sends back a signal to Sink
else
sends back a normal response packet
end if
end for
if Sink receives a collection of the reply packet
if an intermediate node does not send back a    response
Sink records the identity of that intermediate node
end if
Sink analyzes the status information of the nodes on the routing path
Sink finds out the malicious nodes
Sink broadcasts the identity of malicious nodes
end if
end for
```

The network set up energy by transmitting packets, receiving packets, overhearing, switching energy, and sensor logging. The nature of the sensor nodes determine the processes involved in consuming energy. For example, the sink node need not participate in overhearing and hence, it does not absorb energy in overhearing of packets from neighboring nodes.

3.3 Detection Based on RAELPM

Base Station monitors each node included in the suspicious set. BS sends a HELLO request to both suspicious node and its neighbors in the neighbor list. If the node along with its neighbors replies to the Base station then that node is not a wormhole and is considered to be genuine. If reply does not come from the neighbors then it is confirmed that they do not belong to that network and so they need to be malicious. This confirms the presence of a wormhole link in the network. The property of the malicious node is that it can limit its transmission power and deceive the RAELPM detection. The proposed algorithm helps to detect such misbehaving nodes exactly. A simple case is taken to analyze the proposed algorithm to find the accuracy of detecting the malicious node and thereby eliminating the limitation of RAELPM detection mechanism.

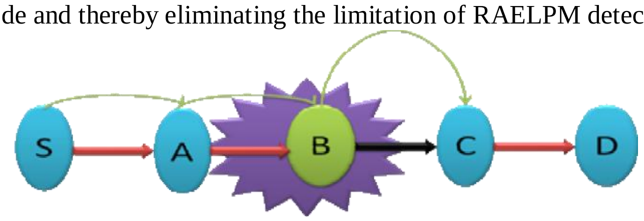


Figure 3.1 Scenario of node B limiting its transmission power

Figure 3.1 depicts the scene of a malicious node limiting its transmission control. The source node is S, the destination is D, and the others are the intermediate nodes. In the mechanism, when B limits its transmission power, it makes the RAELPM detection believe that the packet has been sent. The packet gets dropped without the destination receiving it.

It assumes that the receiver has received the packet and declares the malicious node to be valid node and in the process, the right node C is falsely reported as malicious (instead of B). This false misbehavior detection is eliminated in the proposed technique. In this method, the responses from the RAELPM detection mechanism are considered as the response packets for the sink node. The packets are sent through the nodes in the network. A list of status bits is kept for the nodes on the routing path after the sink receives all the response packets from them within a limited time cycle.

The status for one round of reply can be denoted by a vector, … , , 1 ,0 , 1 . The sink can perform intrusion detection by analyzing the status vector. To any, if 0 or -1 and 1, then is a change point in B. A change point is a sensor node on the routing path where the value of status bit turns from 0 or -1 to 1. If a node is a suspicious point and is the nearest downstream node on the routing path, then the sequence, contains a malicious node. The major goal of the proposed algorithm is to find those smallest malicious sequences on the routing path. The lowest malicious sequence always includes a suspicious point as well as the nearest downstream node of the questionable point.

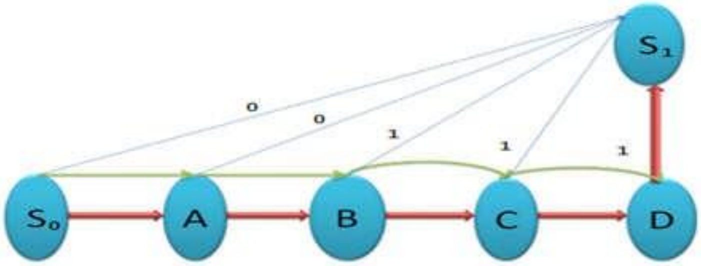


Figure 3.2Implementation of the proposed algorithm

The smallest malicious sequence can be found by detecting the suspicious point as well as the nearest downstream node which contains a malicious node. The implementation of the proposed algorithm is shown in Figure 3.2. It shows the response bits of one round of the source node and the intermediate nodes A, B, and C being sent to the sink node.

Algorithm:

Let – Source node;, … … – Input node; – Sink node; - Malicious node

```
for each   watches   whether data sent successfully or not
At the same time   sends the data to the
if is a true node
response bit of   is zero
else
response bit of   can send zero or one
end if
end for
When it reaches all the response bit will be sent to By fixing the suspicious point, the exact will be found out.
```

A suspicious point is set for the node which has the previous status bit as 0 or -1 and if there is a transition to 1 in subsequent data collection. Thus, the sensor node on the routing path for which the value changes from 0 or -1 to 1 is referred as the suspicious point (from both downstream and upstream path). Implementation of this concept in the existing RAELPM detection mechanism enhances the performance by eliminating the misbehaving node accurately. Without such measure, the process becomes high time to consume and energy inefficient.

4. 4.Result and Discussion

The proposed RAELPM detection approach has been implemented in Network simulator NS2. We have designed network topology with different scenarios with a different number of nodes. The proposed methodology has been evaluated with different density networks with multiple malicious nodes. The following table 1 shows the simulation parameters used to evaluate the proposed method. NS-2 has written using C++ language, and it uses Object Oriented Tool Command Language (OTCL). It came as an extension of Tool Command Language (TCL). The simulations were carried out using a WSN environment consisting of 71 wireless nodes over a simulation area of 1000 meters x 1000 meters flat space operating for 60 seconds of simulation time. The radio and IEEE 802.11 MAC layer models were used.

Table 1 The parameters used in our simulation

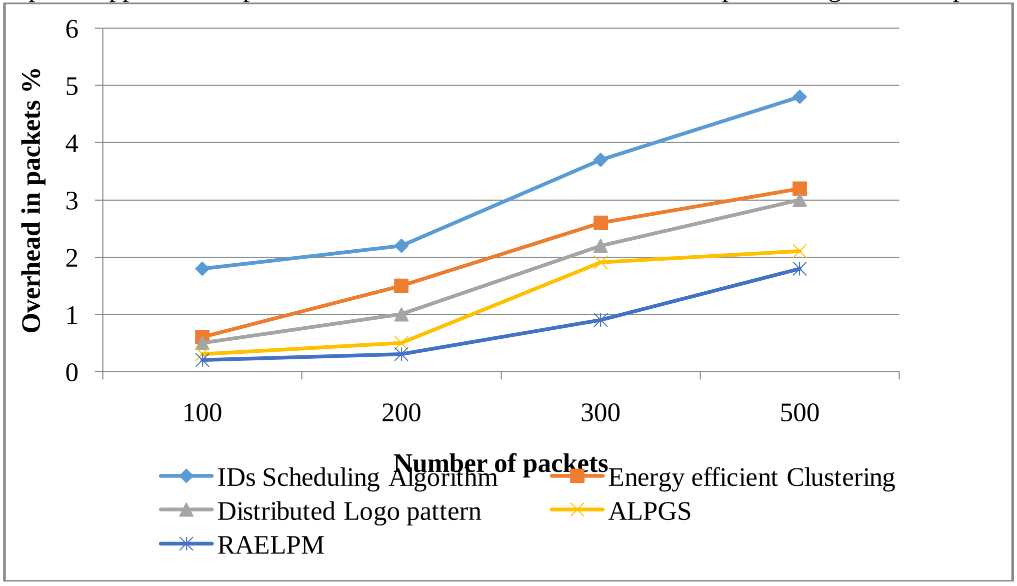
Parameters	**Value**
Version	NS-alone 2.28
Area	1000m x 1000m
Transmission Range	250 m
Traffic model	UDP, CBR
Packet size	512 bytes

Table2: shows the comparison results

S. No	Number of Nodes	Protocol	Detection Rate		Throughput	PDF
			False +ve	**False -ve**		
1.	71	IDs Scheduling Algorithm	3.5	2.5	92	86.70
2.	71	Energy efficient Clustering	0.9	0.8	97.8	93.50
3.	71	Distributed Logo pattern	0.7	0.6	98.2	95.30
4.	71	ALPGS	0.5	0.3	99.1	96.80
5.	71	RAELPM	0.3	0.1	99.65	98.28

4.1 Intrusion Detection overhead Performance:

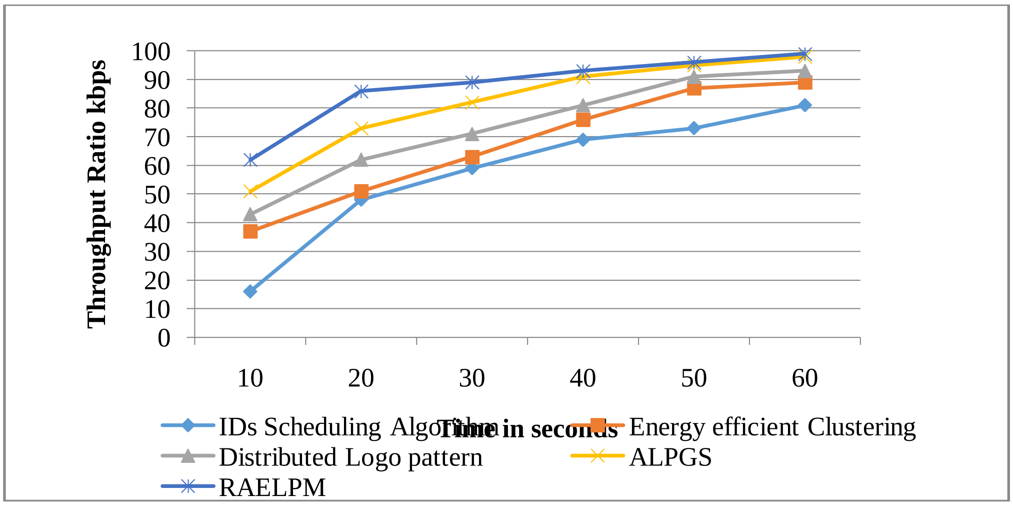
The overhead generated by the routing attack detection process has been shown in graph1. It indicates that the proposed approach has produced less cost than other methods while performing detection process.



Graph1 shows the value generated by intrusion detection.

4.2 Throughput performance

Throughput is the rate of packets received at the destination successfully. It is usually measured in data packets per second or bits per second (bps). Average throughput can be calculated by dividing the total number of packets received by the entire end to end delay.

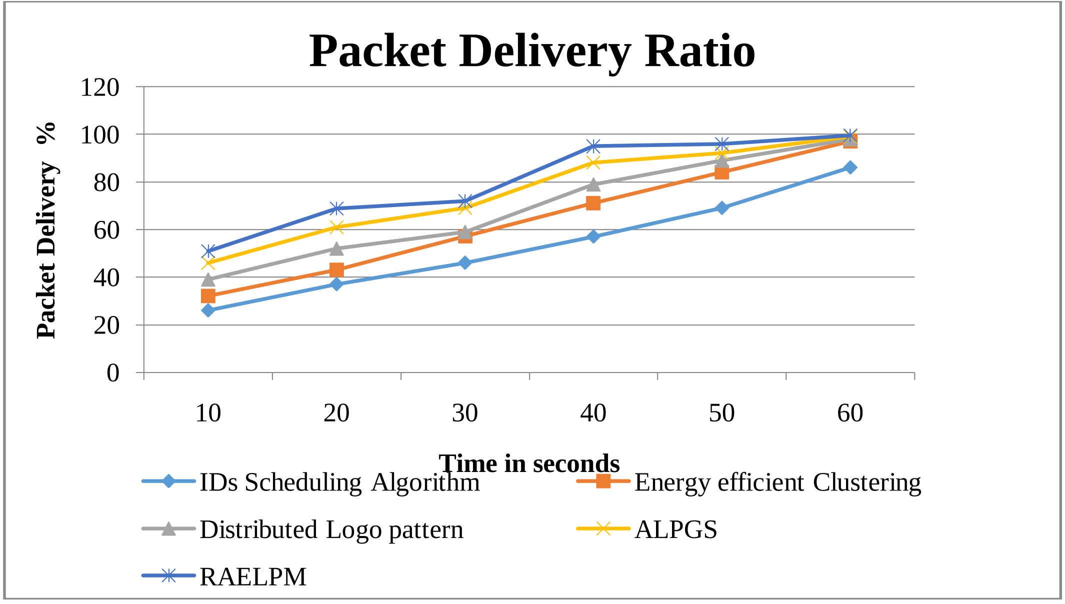


Graph.2 Throughput ratio of different methods

The Graph2 shows the overall performance ratio of different methods, and it is clear that the proposed method has achieved higher throughput than other methods.

4.3 Packet Delivery Fraction:-

The packet delivery ratio defines the rate of data packets received at a destination according to the number of packets generated by the source node. The packet delivery ratio (PDF) is computed as follows.
PDF =(No. of Packets Received/No. of Packets Sent)*100.

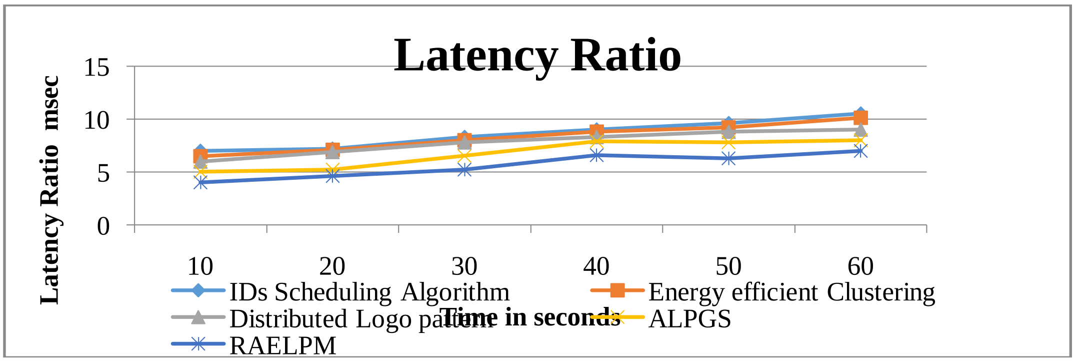


Graph3: Packet Delivery Ratio

The Graph 3: shows the performance of packet delivery ratio of different algorithms and it indicates that the proposed Flow-based method has higher packet delivery ratio than other methods.

4.4 Average End-to-End delay:-

Average end to end delay includes all possible delay caused by buffering during route discovery latency, queuing at the interface queue, and delay at the MAC due to retransmission, propagation and transfer time. Its overall time is taken for a data packet to be transmitted across the sensor network from source to destination.



Graph4: End-to-end delay

Delay = t_R - t_S
Where t_R is the receiving time, and t_S is the sent time.

The Graph4 shows the latency ratio of different methods, and it shows clearly that the proposed method has lower latency rate than others.

5. Conclusion:

An RAELPM intended to detect IDs and misbehaving malicious node. It becomes mandatory to identify these nodes to prevent the network from loss or tampering of packets. Optimization of energy in the case of WSN is much more intricate than conventional RAELPM techniques because it engages in not only reducing the consumption of energy of a single sensor node but also in maximizing the lifetime of an entire network. This work has taken both the criteria of detecting the malicious node accurately and optimize the lifetime of the system into consideration. Also, it is found that the technique proposed detects the malicious node accurately whereas the existing method fails to identify it correctly. The reduction in energy consumption for the network setup proves to be very significant for WSN. Our proposed approach comes very handily even with densely deployed networks. In this work, we focused on detecting the presence of a single IDs node in the network.

References:

[1]. Alan Dahgwo Yein & Chih-Hsueh Lin 2017, ‘A Secure Mutual Trust Scheme for Wireless Sensor Networks’ IEEE, Vol 12.

[2]. Abdusy Syarif & Riri Fitri Sari 2011, ‘Performance analysis of AODV-UI routing protocol with energy consumption improvement under mobility models in hybrid ad hoc network’, International Journal of Computer Science and Engineering, vol. 3, no. 7.

[3]. Agarwa PK, Gupta BB, Jain S & Pattanshetti MK 2011, ‘Estimating strength of a DDoS attack in real time using ANN based scheme’, Communications in Computer and Information Science, Springer, vol. 157, pp. 301-310.

[4]. Ahmed R & Mahlous D 2015, ‘A framework against DDoS in a multipath network environment’, Scientific research publishing, Communications and network, vol. 7, pp. 106-116.

[5]. Akbani R, Korkmaz, T & Raju, GVS 2012, ‘Mobile ad-hoc network security’, Journal of electrical engineering, New York: Springer, vol. 127. pp. 659-666.

[6]. Akbani, RH, Patel, S & Jinwala, DC 2012, ‘DoS attacks in mobile ad-hoc networks a survey’, in Proc. 2nd International Meeting ACCT, Haryana, India, pp. 535-541.

[7]. Alomari, E, Manickam, S, Gupta, BB, Karuppayah, S &Alfaris, R 2012, ‘Botnet based DDoS attacks on web Servers: Classification and art’, International Journal of Computer Applications, vol. 49, no. 7, pp. 24-32.

[8]. Amit Kumar Singh 2015, ‘Identity-Based Key Distribution for Wireless Sensor Networks using Cryptographic Techniques’, International Journal on Emerging Technologies, ISSN 0975-8364, vol. 6(1), pp. 69-72.

[9]. Andrew, C, Mohammad, H & Omar, A 2015, ‘Defence for DDoS attacks in cloud computing’, International conference on advanced wireless, Information, and Communication Technologies, vol. 73, pp. 490-497.

[10]. Annapurna P Patil, Rajanikanth, K, Bathey Sharanya, MP, Dinesh Kumar & Malavika, J 2011, ‘Design of an energy efficient routing protocol for MANETs based on AODV’, IJCSI International Journal of Computer Science Issues, vol. 8, no. 1, pp. 4.

[11]. Anwar Ghani & Husnain Naqvi 2015, ‘An efficient signcryption scheme with forward secrecy and public verifiability based on hyper elliptic curve cryptography’, Multimedia Tools and Applications, vol. 74, no. 5, pp. 1711-1723.

[12]. Arun Kumar & Rajeshwar Singh 2011, ‘Mobile Ad Hoc Networks Routing Optimization Techniques using Swarm Intelligence’, IJRIM, ISSN 2231-4334, vol. 1, no. 4, pp. 13-33.

[13]. Arvind, S Kamble & Deepika D Patil 2016, ‘Routing Protocols for Wireless Sensor Networks’, International Journal of Advance Engineering and Research Development, ISSN 2348-6406 vol. 2, Issue 5.

[14]. Asha Nagesh 2008, ‘Distributed Network Forensics using Jade Mobile Agent Framework’, Arizona State Unicversity.

[15]. Asokan, R 2010, ‘Ant Based Dynamic Source Routing Protocol to Support Multiple Quality of Service (QoS) Metrics in Mobile Ad Hoc Networks’, International Journal of Computer Science and Security, vol 2, Issue 3, pp. 48-56.

[16]. Baojiang Cui & Ziyue Wang 2015, ‘Enhanced Key Management Protocols for Wireless Sensor Networks’, Mobile Information Systems, Article ID 627548, 10 pages.

[17]. Baquero, C, Almeida, P, Menezes, R & Jesus, P 2012, ‘Extrema propagation: Fast distributed estimation of sums and network sizes’, IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 4, pp. 668-675.

[18]. Belenky, A & Ansari, N 2003, ‘IP Traceback with Deterministic Packet Marking’, IEEE Communication, vol. 7, no. 4, pp. 162-164.

[19]. Bertier, M, Mostefaoui, A & Trédan, G 2011, ‘Low-cost secret-sharing in sensor networks’, in Proceedings of the IEEE 12th International Symposium on High Assurance Systems Manufacturing (HASE '10), pp. 1-9.

[20]. Chaitanya Buragohain 2015, ‘Anomaly based DDoS Attack Detection’, International Journal of Computer Applications, vol. 123, no. 17.

[21]. Chang Lung, T, Chang, AY & Ming Szu, H 2010, ‘Early warning system for DDoS attacking based on multilayer deployment of time delay neural network’, Proceedings of IEEE 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 704-707.

[22]. Chen, CL 2009, ‘A New Detection Method for Distributed Denial of Service Attack Traffic based on statistical test’, Journal of Universal Computer Science, vol. 15, pp. 488-504.

[23]. Chen, Y, Hwang, K & Ku, W 2007, ‘Collaborative Detection of DDoS Attacks Over Multiple Network Domains’, IEEE Transaction on parallel and distributed systems, vol. 18, no. 12, pp. 1649-1662.

[24]. Chen, Z, Chen, Z & Delis, A 2007, ‘An Inline Detection and Prevention Framework for DDoS Attacks’, Computer Journal, pp. 27-40.

[25]. Chi Chun, L 2010, ‘A Cooperative Intrusion Detection System Framework for Cloud Computing Networks’, In Parallel Processing Workshops, 39th International Conference, pp. 280-284.

[26]. P. Richtárik and M. Takáˇc, “Iteration complexity of randomized blockcoordinate descent methods for minimizing a composite function,” Math. Program. A, vol. 144, no. 1, pp. 1–38, Dec. 2012.

[27]. S. Boyd and L. Vandenberghe, Convex Optimization. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[28]. P. K. Gopala, L. Lai, and H. El Gamal, “On the secrecy capacity of fading channels,” IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[29]. Z. Li, R. Yates, and W. Trappe, “Secret communication with a fading eavesdropper channel,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2007, pp. 1296–1300.

[30]. J. Li and A. P. Petropulu, “On ergodic secrecy rate for Gaussian MISO wiretap Y. Liang, H. V. Poor, and S. Shamai (Shitz), “Secure communication over fading channels,” IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.