Energy Adaptive Intrusion Detection System for Energy Harvesting IoT

S.Prabavathy, J.S.Kanchana

Abstract: ***Internet of Things (IoT) is an emerging technology that makes network of physical objects which can identify, communicate and share information through Internet. The edge of IoT network are mostly simple sensors. The success of the IoT application depends on the quality of sensor data at the right time, this leads to the requirement of IoT devices be long term, self-sustaining and have the ability to harvest their required energy from deployed environment. Such devices incur additional security challenges because of prolonged life time and change in the life cycle of devices. A novel intrusion detection system is designed for energy harvesting 6LoWPAN based IoT network considering the energy scavenging characteristics of devices in addition to conventional IoT. The simulation results confirm that the proposed intrusion detection system is efficient and accurate in detecting the attacks.***

Keywords: Energy harvesting, Intrusion Detection System, Internet of Things, 6LoWPAN, RPL.

I. INTRODUCTION

The Internet of Things (IoT) is a global network of smart objects called 'things' embedded with electronics, sensors and software. The evolution of IoT makes billions of devices to be connected in the dynamic network to provide intelligent applications for supporting human in applications such as environmental monitoring, healthcare, logistics, security and surveillance [1]. IoT is made up of new revolutionary technologies providing combinations of ubiquitous and pervasive environment to human. To realize such an environment wireless sensor networks (WSN) are used which is battery powered. As the number of wireless nodes increases, number of batteries also increases which leads to the problem of increased production, proper maintenance and disposal of these batteries [2]. Energy harvesting mechanism provides a better solution to solve this problem at many instances.

To provide low cost IoT applications, the sensor nodes must incur low cost and involve low maintenance. Though the advancement in the field of electronics has led to the design of sensors with low power requirements, cannot satisfy the increasing demand of wireless sensor network applications. This results to development of energy harvesting sensors. These energy harvesting sensors has the capability to extract the required energy from the deployed environment. The harnessing energy from ambient light, vibrations, thermal gradients and other forms of motion is converted into electrical energy to power up the node [3].

Low cost IoT applications have limited power and memory, this leads to the requirement of communication protocol which can efficiently manage the resource constrained devices. 6LoWPAN provides solution to efficiently manage the low cost IoT application. The 6LoWPAN can be implemented using energy harvesting sensors. 6LoWPAN consist of adaptation layer in network protocol stack to integrate IPv6 into low power networks such as IEEE 802.15.4. This provides the advantage for existing IP network to use the address space and infrastructure of IPv6. The 6LoWPAN is connected to the internet through the border router. The border router handles the data communication within the network and in the Internet. RPL (Routing Protocol for Low Power and Lossy Network) is the routing protocol for 6LoWPAN. In 6LoWPAN security threats can be from both Internet through adaptation layer and within the 6LoWPAN network. The security mechanism in RPL can detect external threats only, but not the internal threats [4].

The energy harvesting capability of the sensor nodes increases the lifetime of sensor nodes. This lead to the change in the life cycle of sensor node which provides new security challenges to WSN [5]. In regular 6LoWPAN the compromised sensor nodes run out energy and stop its attacks at some instant of time, but in energy harvesting network the attack continues, since the life time of the sensors are prolonged. Therefore, security solutions designed for regular 6LoWAPN is not sufficient for energy harvesting 6LoWPAN. A new security mechanism has to be designed considering the energy scavenging characteristics of the sensor nodes in 6LoWPAN. Intrusion detection system (IDS) is the first layer of defense from the adversary in WSN. In this paper, a novel intrusion detection mechanism is proposed in order to provide security to energy harvesting IoT based on the energy availability of the nodes.

The remainder of the paper is organized as follows: Section 2 briefly discuss the security requirements of energy harvesting IoT. Section 3 provides a brief introduction to the 6LoWPAN based IoT network. Section 4 overviews the related work and compares the proposed system with existing works. Section 5 describes the design of the proposed Energy

Revised Manuscript Received on December 05, 2019

***** Correspondence Author

Dr.S.Prabavathy*, Department of IT, G.Narayanamma Institute of Technology & Science , Hyderabad, India.

Dr.J.S.Kanchana, Department of IT, K.L.N. College of Engineering, Madurai , India.

adaptive intrusion detection system. Section 6 provides the simulation and results of the proposed work. Section 7 summarizes of the proposed system.

II. SECURITY OBJECTIVES OF ENERGY HARVESTING IOT

The security mechanisms in an energy harvesting WSN should protect the data transmitted over the network from attacks of malicious nodes along with energy scavenging activities. The essential security objectives of energy harvesting IoT are listed below:

A. Integrity

In conventional system integrity is protection against unauthorized modification and tampering of object's identity and their data. In context of Energy Harvesting IoT integrity is extended to protect against any kind of impersonation, data modification along with energy level modification. Some of the attacks against integrity are Sybil attacks, defamation etc.

B. Confidentiality

The security mechanism should ensure that a node should allow only authorized access to its data. In the context of Energy harvesting IoT confidentiality is extended to protect the energy information of each node along with the data. The various types of attack against confidentiality are Man-in-middle attack, traffic analysis attack, etc.

C. Availability

The security mechanism should ensure that the services should be available always available. In the context of Energy Harvesting IoT, availability should ensure data availability and energy availability. The legitimate devices should be always available for service. These malicious devices can disrupt the possibility to communicate with the legitimate devices. The various types of attack against availability are Denial of Service, selective forwarding, black holes etc.

III. BACKGROUND

In this section a brief introduction to various technologies of 6LoWPAN is provided.

A. IoT implementation using 6LoWPAN

IoT is made up of millions of devices connected in a network. 6LoWPAN is specialized task group formed by Internet Engineering Task Force (IETF). It provides efficient communication between the sensor nodes using IPv6 over a network of resource constrained devices [6]. 6LoWPAN uses Internet Protocol version 6 (IPv6) as networking protocols and RPL as routing protocols. It supports multi-hop routing among sensor nodes connected to 6LoWPAN Border Router (6BR). The 6BR is an end device which connects the sensor network with the Internet and performs the communication between IPv6 and 802.15.4 interfaces. 6LoWPAN is a multihop wireless network of lossy communication link with specialized routing protocol and operating system based on its specification. Contiki [7] is one of the open source operating system that supports 6LoWPAN based IoT application with multithread and multitasking environment.

B. RPL

IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) is routing protocol specially implemented for low power and lossy networks such as 6LoWPAN. It supports point-to-point (P2P), point-to-multipoint (P2MP) and multipoint-to-point (MP2P) communications. RPL routing protocol builds a Destination Oriented Directed Acyclic Graph (DODAG) topology with 6BR as its root. Each DODAG has unique identifier and it can be optimized using Objective Function that uses particular metric for optimizing the route. The objective function is represented by Objective Code point which uses the metrics such as energy, hop count, latency etc. [8] for route optimization. Each node in the DODAG is assigned a rank that determines its relative position and distance to 6BR. An example DODAG topology of 6LoWPAN is shown in Fig 1.

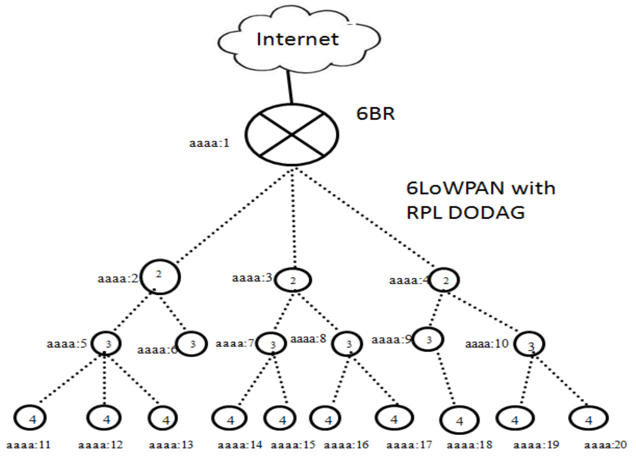

Fig .1. Sample 6LoWPAN RPL topology

C. Security Challenges in energy harvesting 6LoWPAN

The security requirement of IoT varies from one application to another due to emergence decentralization in its architecture. This requirement leads to many security challenges in IoT. The IPsec protocol [9] provides end-to -end security for IPv6 communication and IEEE 802.15.4 link layer provides hop-by-hop security. These protocols provide message security and not the network security. The 6LoWPAN is vulnerable to numerous attacks [10] and the energy harvesting characteristics increases strength of the attack. Therefore an efficient intrusion detection mechanism is required for energy harvesting 6LoWPAN to protect the network from active and passive attack.

IV. RELATED WORK

Various researches have been performed in security requirements of IoT [11][12][13]. The co-existence of wireless sensor network and Internet in 6LoWPAN provides numerous security challenges. Various attacks against 6LoWPAN and RPL have been studied in [14][15][16]. The research area of IoT intrusion detection is very young and only very few works have been performed in it. Signature based intrusion detection system proposed in [17] provides detection mechanism for resource constrained sensor network. The signature matching mechanism for attack detection proposed in this consumes more power of sensor nodes.

The work proposed by [18] is an attack detection architecture built on the top of ebbits network. It can detect only the DoS attack and this architecture is specific only to ebbits network. The IDS proposed in [19] is a combination of distributed and centralized intrusion detection mechanism for 6LoWPAN. This detects the attack based on RPL DODAG topology inconsistency. It uses the centralized module called 6Mapper placed at 6BR to build the current network RPL topology and detects the inconsistency. Since detection mechanism is centralized it incurs more energy and delay in detecting the attack.

The IDS given in [20] is used to detect the wormhole attack in 6LoWPAN at non-leaf nodes of RPL DODAG topology. This mechanism cannot detect attack occurring at the leaf nodes of RPL DODAG topology. A specification based IDS were given in [21] which detect only the RPL topology attacks. Many clustering based IDS mechanisms [22][23][24] have been proposed for wireless sensor networks, which detects the intrusion. These mechanisms are not suitable for 6LoWPAN which routes the traditional Internet traffic into WSN. The threat model and taxonomy of attacks for energy harvesting WSN was studied in [5] which provides only the conceptual overview.

The above mentioned intrusion detection systems does not consider the security issues involved in energy harvesting characteristics of the sensors. The proposed IDS for energy harvesting 6LoWPAN based IoT is distinct from all the above works in providing an energy adaptive intrusion detection approach.

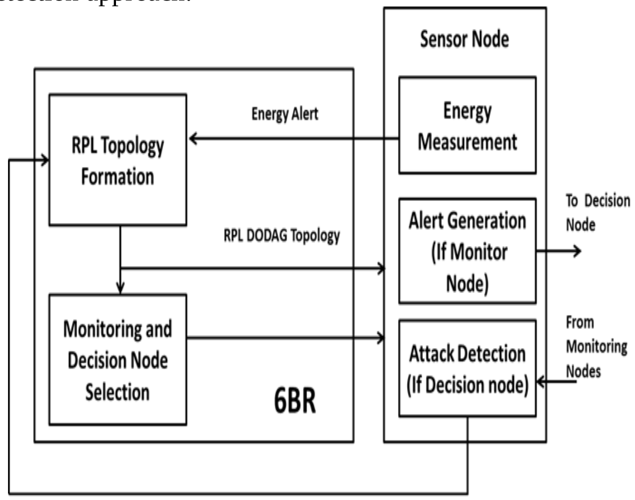

Fig. 2. Functionalities of the proposed IDS for energy harvesting 6LoWPAN

V. ENERGY ADAPTIVE INTRUSION DETECTION SYSTEM

The proposed Energy Adaptive Intrusion Detection System (EAIDS) is an agent based distributed collaborative approach designed for energy harvesting 6LoWPAN networks. In this approach attack is detected by the IDS agent at the nodes based on the abnormality behavior of the nodes. The intrusion detection agent will be implemented in the 6BR and in all sensor nodes. The IDS agents are activated only when the energy level is sufficient to handle intrusion detection process. The agents in nodes are used to detect the attacks locally and transmit the alert message only when the attack is detected, thus reducing the communication overhead. 6LoWPAN uses RPL as routing protocol and creates a DODAG tree topology with the parent-child relationships among the sensors and border router 6BR as the root of the tree. In EAIDS, the IDS agent of a node will monitor the nodes where it has a direct relationship with them, i.e. its parents or its children, instead of monitoring all its neighboring nodes. The detection results are compared locally at the decision nodes and final decision about suspicious node is made. Thus, the attack is detected at faster rate than in centralized system. The information about the malicious node is sent to the 6BR to update the RPL topology. Based on the energy level of the nodes, monitoring and decision nodes are selected. The energy level of each node is obtained and stored by 6BR before the construction of DODAG topology. The operations performed by the proposed IDS are shown in Fig 2. The 6BR which is the root of RPL DODAG does not require monitoring nodes because it is a high computing device that can protect itself using the any cryptographic measures. The leaf node has variant of monitoring node selection method and detection mechanism from non-leaf node. The overall activities of the proposed IDS are given in Algorithm1.

Algorithm 1: EAIDS

```
At 6BR:
        RPL DODAG Topology Construction
        Monitoring_Node_Selection(node)
        Decision_Node_Selection(node)
At Sensor Nodes:
   if (Energy(node) > Energy_Threshold )
        While(detection window W)
        Alert_Generation(Monitoring Node)
        Attack_Detection(Decision Node)
        End while
    Else
        Create(energy_alert)
        Forward(energy_alert to 6BR)
    End if
End
```

A. Monitoring Node and Decision Node Selection

In order to reduce resource consumption, certain IDS agents are only activated for monitoring instead of making all IDS agents to involve in the monitoring process. Every node of 6LoWPAN maintains preferred parent list containing next possible parents based on the objective function of RPL routing topology. EAIDS uses this list to activate the IDS agent. To monitor a non-leaf node, its children nodes preferred parent list is analyzed to identify the nodes which has at least one common preferred parent with the energy level above the threshold. The IDS agents in these nodes are activated for monitoring the parent node and it is treated as monitoring nodes.. Similar to non-leaf nodes, to monitor the leaf nodes, its sibling nodes preferred parent list is used to find the monitoring node. The selection of monitoring nodes is given in Algorithm-2

Algorithm 2:
Monitoring_ Node_Selection(DODAG topology)

```
Require: RPL DODAG Topology
For each node in DODAG topoplogy

// selecting nodes with common preferred parent list

   For each non-leaf  node j except root     //  for non-leaf node
        chlist=Getchildren(j)
             For each node c in chlist
              If((preferedparent(c) ∩
            preferedparent(c+1))≠NULL)
   Nodes_With_common_parents(j) = c U c+1
              End if
   End for
    End for

    For each leaf  node j          // for leaf node
            Sblist=GetSibling(j)
            For each node g in Sblist
               If(preferedparent(g) ∩
            preferedparent(g+1))≠NULL)
                     Nodes_With_common_parents(j) = c U c+1
     End if
     End for

//Veryfing energy levels of the above selected nodes
    For each node d in Nodes_With_common_parents
       If(Energy(d) > Energy_Threshold )
      Monitor(j)=d
       End if
    End for

//If the nodes selected is more than half of the number of child or sibling then the nodes with more number of common preferred parent is removed

    If(count(Monitor(j) > count(chlist(j))/2+1 ||
          While(count(Monitor(j)=count(chlist(j))/2+1))
        n = nodes with highest common preferred parent
                  Monitor(j)=monitor(j) - n
           End while
    End if

    // if the selection return null then all the children or siblings are made as monitor

        If(Monitor(j)= ϕ)
           Monitor=chlist or sblist
        End if
End for
```

The energy for communicating all the data from monitoring node to centralized 6BR for decision making about intrusion is high, so decision making is performed locally. The nodes which perform the decision making about intrusion based on data from monitoring nodes are called decision nodes. Decision nodes are selected by 6BR based on the current energy level and RPL topology. The 6BR selects the one of common preferred parent of each set monitoring nodes as decision node. Sometimes a node can be both monitoring node for its parent and decision node for its child nodes. Algorithm 4 is used for selecting the decision node. The monitoring nodes and decision nodes are treated as regular sensor node by the next level nodes of RPL topology and monitored for any malicious activity. After the selection of monitoring nodes and decision nodes it is updated to the sensor nodes by 6BR. A sensor node which receives this information activates its IDS to monitor or to make decision about intrusion.

Algorithm 3:
Decision _Node_Selection(DODAG topology)

```
Require: RPL Topology
      For each node j in Monitor
         x = maximum occurred node in
                (preferedparent(j) ∩
                               preferedparent(j+1))
         if(Energy(x) > Energy_Threshold)
            Decider =x
         end if
     End for
```

B. Alert Generation by Monitoring Nodes

A detection window of size w units is used in EAIDS for performing monitoring and decision making. The IDS agent in monitoring node, observes the overheard packets for w period. If it identifies any abnormal behavior, it sends alert message to its decision nodes. The IDS agent in the monitoring node generates alert message if the observed security parameter value crosses the threshold criterion. This process is given in Algorithm 5. The process is repeated for every window of size w. The overall working of EAIDS is shown in Fig. 3, where MN are monitoring nodes and DN are decision nodes.

Algorithm 4:Alert_Generation(node)

```
While( indow w)
    If (security parameter <> threshold)
        Drop (packet)
       Create(security_alert)
       Send(security_alert to decision node)
    Else
       Forward(packet)
End while.
```

C. Attack Detection by Decision Nodes

The IDS agent in the decision nodes after receiving alert message it decides about the intrusion and sends its decision to 6BR for RPL topology updating. If more than half of the monitoring nodes have raised an alert, then the parent node is considered to have abnormal behavior and IDS agent declare it as malicious node. The procedure for attack detection is given in Algorithm 6.

When the IDS agent in the monitoring node ascertains the abnormal activity it will issue alert message to the decision nodes. The IDS agent in the decision nodes makes the final decision associated with the abnormal behavior of the parent based on alert messages received from the monitoring nodes and send its decision on attack to the 6BR for topology updating. The IDS agent in the monitoring nodes at the leaf level of the RPL DODAG tree not only monitors its parent but also its siblings. When an abnormal activity of sibling node is determined, it will send the alert message to its decision node. Similar process to non-leaf nodes, the decision about alert is performed.

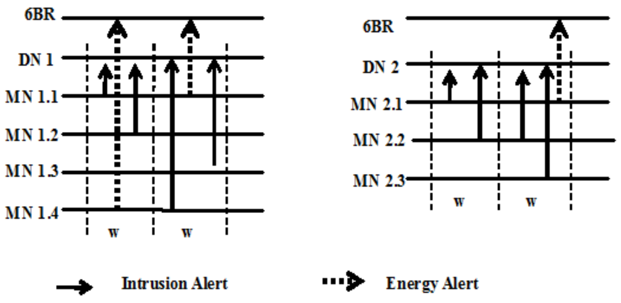

Fig. 3. Alert generation process

Algorithm 5:Attack_Detection(node)

```
While(window w)
  If(Alert messages are from more than half of the monitoring nodes) then
    Send(attack_message to 6BR)
  Else
    Drop(Alert)
  End if
End while
```

D. Energy Adaptation

The proposed IDS is energy adaptive in detecting the attacks. The difference in the stored harvested energy and energy consumed at any instance of time should be always greater than the specified threshold α. If it falls below the threshold then energy alert is generated by that node and sent to the 6BR. If the energy_alert is generated from the monitoring or decision node then 6BR stops that node to perform monitoring or decision activities and selects new monitoring and decision nodes based on RPL DODAG topology. The equation (1) measures the energy of the node at any instance of time were E_h is the harvested energy and E_c is the consumed energy

$$Energy\ (node) = \int_0^t E_h - E_c\ (dt) \qquad (1)$$

The energy of a node $Energy(node)$ should be always greater than the Energy_Threshold α else energy alert will be sent to 6BR and the node will initiate energy harvesting process.

$$Energy(node) > \alpha \qquad (2)$$

E. Selective Forwarding Attack

6LoWPAN is a multi-hop network that forwards data through the participating nodes. These participating nodes may selectively reject certain data [9] reaching the destination. The proposed IDS can efficiently detect such attack. In the proposed IDS, the IDS agent in the monitoring nodes observes the packet dropping rate of its parents to detect this attack. Let PD(Xij) be the packet dropping rate of node i detected by the monitoring node j during the window w. Let β be threshold assigned for packet dropping rate of a node. The monitoring node j sends alert message to its decision node when PD(Xij)>β. When the IDS agent in the decision nodes receives same alert message from more than half of its monitoring nodes about the node i, then the decision node concludes that node i as malicious node. This decision is conveyed to 6BR to remove the node i from DODAG and to reconstruct the DODAG topology. This mechanism can also be used to detect the black hole and worm hole attacks by assigning appropriate thresholds.

F. Version Number Attack

Node disconnection is more frequent in 6LoWPAN due to worst link state or lack of battery power. To handle the disconnections, RPL contains local and global repair mechanism. Local repair use the temporary route through neighbor node with same rank or select next preferred parent where as in global repair mechanism, the entire DODAG is rebuilt. The global repair involves more control messages in DODAG construction which in turn incurs more energy and network resources. Malicious node increments the version number included in the control messages sent by its parents. When these control messages propagated into the network leads to forced rebuild of RPL DODAG topology which results in largest energy depletion. The monitoring node verifies the DODAG version number of each control packet that is received and forwarded by its parent. If there is any change in version number it generates alert to the decision node. When a decision node receives such a alert it immediately sends the attack message to 6BR to remove malicious node from the RPL Topology.

VI. SIMULATION AND ANALYSIS

The experiments are performed in Cooja [25] simulator which uses Contiki operating system. Cooja simulator does not have energy harvesting sensor model hence a simple energy harvesting sensor model is designed using the Tmote Sky sensor nodes. Unit Disk Graph Medium, the Cooja's default lossy radio model is used for transmission. 6BR is not a constrained node and it can be PC or equivalent; however currently there exist no PC equivalent 802.15.4 devices, therefore we run the 6BR natively i.e. on Linux. Five different configurations are used with 16, 24, 32, 40, 48 nodes. Fig 4 shows the sample configuration with 32 nodes. The 6BR selects the monitoring and decision nodes for each configuration. Each experiment is performed 10 times, the mean and standard deviation for each measured value is calculated to maintain the accuracy of the result. Cooja does not have energy harvesting sensor model, so to simulate 6LoWPAN with energy harvesting sensors, a simple energy harvesting sensor model is developed for Tmote Sky nodes. The initial battery level of the node is assigned 300mAh.

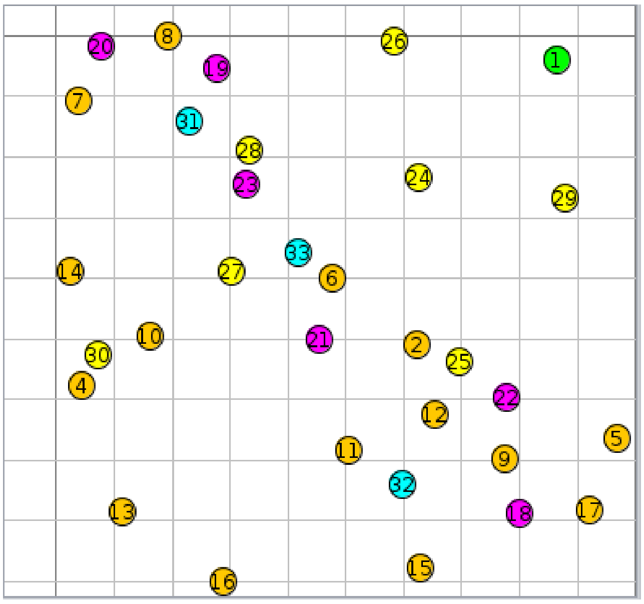

Fig. 4. Sample node configuration

The energy harvesting of a node is performed in parallel along with its regular operation. The energy harvesting is initiated when the energy level of the node reaches the threshold of 150mAh. When energy harvesting is initiated, the energy level of the node is increased linearly to 300mAh and stops the energy harvesting process. There is also energy consumption during energy harvesting process which is taken into account to for energy harvesting and it is deducted from the harvested energy.

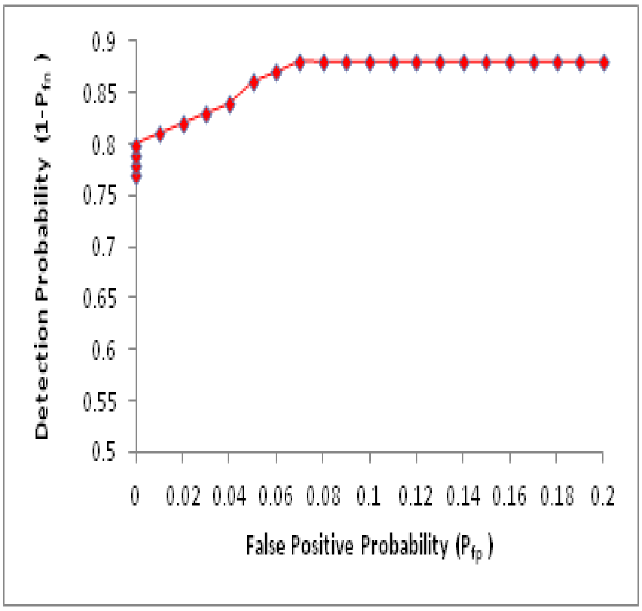

Fig. 5. Detection Probability vs False Positive probability

The proposed IDS efficiently detect the selective forwarding attack. Receiver Operating Characteristic (ROC) curve is used to measure the performance of the proposed IDS. The detection probability i.e. (1- False Negative probability) can be obtained from the ROC with varying false positive probability. The Fig 5 shows ROC of the proposed method, which shows that, as false positive probability increases, the detection probability increases. When the false positive probability reaches zero still the detection probability is high in the proposed method.

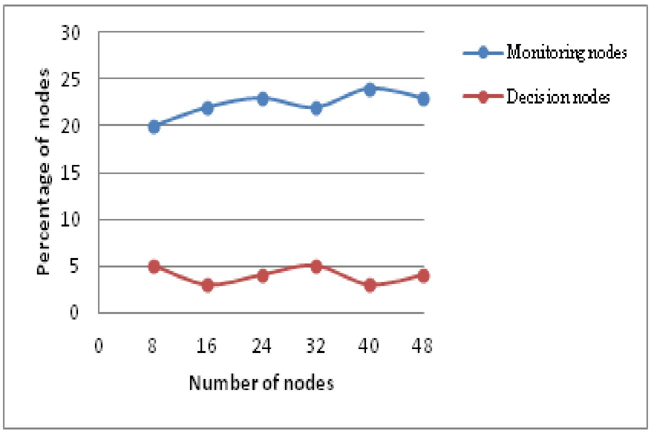

Fig. 6. Percentage of monitoring and decision nodes

The Fig 6 shows the percentage of monitoring and decision nodes selected by the proposed intrusion detection method. The energy consumed by Tmote sky node is calculated using equation (3). To measure the energy consumption by the node Contiki Powertrace [26] application is used.

E_c = [Transmit * Current Consumption: MCU on, Radio TX + Listen * Current Consumption: MCU on, Radio RX + CPU * Current Consumption: MCU on, Radio off + LPM * Current Consumption: MCU idle, Radio off] * Voltage / 4096 * 8 (3)

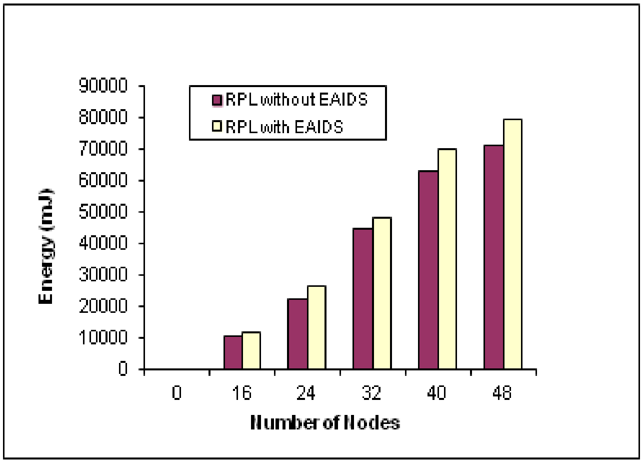

Fig. 7.Energy usage of the network

The Fig 7 shows the network wide energy usage for 30 minutes and Fig 8 shows the energy consumption per node. The results depicts that the proposed EAIDS consumes lesser energy in addition to regular RPL mechanism.

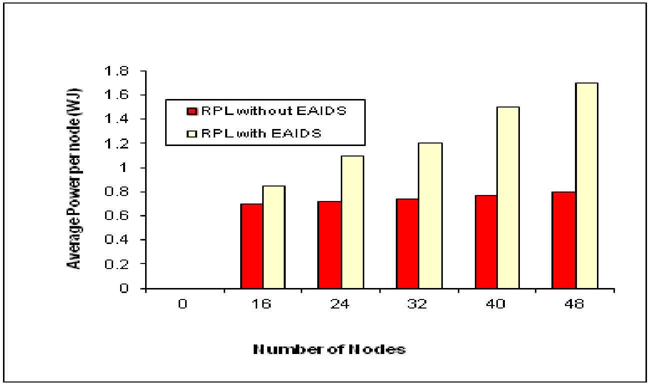

Fig.8. Average Power consumption

VII. CONCLUSION

The impact of the well-known attacks of conventional WSN increases in energy harvesting WSN. Therefore, the proposed Energy adaptive intrusion detection system for energy harvesting 6LoWPAN based IoT is a decentralized system which detects attack locally considering the energy scavenging characteristics of the sensors. The decentralized nature of the proposed system detects attack faster than the centralized system.

The future research is to extend this system to detect more potential attacks that are emerging from Internet of Things. It is also necessary to build a test bed to validate the results of simulation and to increase the performance by tuning the functionalities of the proposed framework.

REFERENCES

1. Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I., 2012. Internet of things: Vision, applications and research challenges. Ad Hoc Networks,10(7), pp.1497-1516.
2. Jain, R. and Wullert II, J., 2002, September. Challenges: environmental design for pervasive computing systems. In Proceedings of the 8th annual international conference on Mobile computing and networking (pp. 263-270). ACM.
3. Priya, S. and Inman, D.J. eds., 2009. Energy harvesting technologies (Vol. 21). New York: Springer.
4. Le, A., Loo, J., Lasebae, A., Aiash, M. and Luo, Y., 2012. 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach. International Journal of Communication Systems, 25(9), pp.1189-1212.
5. Di Mauro, A., Papini, D., Vigo, R. and Dragoni, N., 2012. Toward a Threat Model for Energy-Harvesting Wireless Sensor Networks. In Networked Digital Technologies (pp. 289-301). Springer Berlin Heidelberg.
6. Shelby, Z. and Bormann, C., 2011. 6LoWPAN: The wireless embedded Internet (Vol. 43). John Wiley & Sons.
7. Dunkels, A., Grönvall, B. and Voigt, T., 2004, November. Contiki-a lightweight and flexible operating system for tiny networked sensors. In Local Computer Networks, 2004. 29th Annual IEEE International Conference on(pp. 455-462). IEEE.
8. Hui, J.W., 2012. The routing protocol for low-power and lossy networks (rpl) option for carrying rpl information in data-plane datagrams.
9. Raza, S., Duquennoy, S., Chung, T., Voigt, T. and Roedig, U., 2011, June. Securing communication in 6LoWPAN with compressed IPsec. In Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on (pp. 1-8). IEEE.
10. Hennebert, C. and Dos Santos, J., 2014. Security protocols and privacy issues into 6lowpan stack: A synthesis. Internet of Things Journal, IEEE,1(5), pp.384-398.
11. Weber, R.H., 2010. Internet of Things–New security and privacy challenges.Computer Law & Security Review, 26(1), pp.23-30.
12. Medaglia, C.M. and Serbanati, A., 2010. An overview of privacy and security issues in the internet of things. In The Internet of Things (pp. 389-395). Springer New York.
13. Roman, R., Zhou, J. and Lopez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. Computer Networks,57(10), pp.2266-2279.
14. Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), pp.1645-1660.
15. Pongle, P. and Chavan, G., 2015, January. A survey: Attacks on RPL and 6LoWPAN in IoT. In Pervasive Computing (ICPC), 2015 International Conference on (pp. 1-6). IEEE.
16. Hummen, R., Hiller, J., Wirtz, H., Henze, M., Shafagh, H. and Wehrle, K., 2013, April. 6LoWPAN fragmentation attacks and mitigation mechanisms. InProceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks (pp. 55-66). ACM.
17. Amin, S.O., Siddiqui, M.S., Hong, C.S. and Lee, S., 2009. RIDES: Robust intrusion detection system for IP-based ubiquitous sensor networks.Sensors, 9(5), pp.3447-3468.
18. Kasinathan, P., Pastrone, C., Spirito, M.A. and Vinkovits, M., 2013, October. Denial-of-Service detection in 6LoWPAN based Internet of Things. In 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (pp. 600-607). IEEE.
19. Raza, S., Wallgren, L. and Voigt, T., 2013. SVELTE: Real-time intrusion detection in the Internet of Things. Ad hoc networks, 11(8), pp.2661-2674.
20. Pongle, P. and Chavan, G., 2015. Real Time Intrusion and Wormhole Attack Detection in Internet of Things. International Journal of Computer Applications, 121(9).
21. Le, A., Loo, J., Luo, Y. and Lasebae, A., 2011, October. Specification-based IDS for securing RPL from topology attacks. In Wireless Days (WD), 2011 IFIP (pp. 1-3). IEEE.
22. Kachirski, O. and Guha, R., 2003, January. Effective intrusion detection using multiple sensors in wireless ad hoc networks. In System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on(pp. 8-pp). IEEE.
23. Huang, Y.A. and Lee, W., 2003, October. A cooperative intrusion detection system for ad hoc networks. In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (pp. 135-147). ACM.
24. Sterne, D., Carman, D., Wilson, B., Talpade, R., Ko, C.H., Tseng, C.Y. and Bowen, T., 2005, March. A general cooperative intrusion detection architecture for MANETs. In Information Assurance, 2005. Proceedings. Third IEEE International Workshop on (pp. 57-70). IEEE.
25. Osterlind, Fredrik, Adam Dunkels, Joakim Eriksson, Niclas Finne, and Thiemo Voigt. "Cross-level sensor network simulation with cooja." In Local Computer Networks, Proceedings 2006 31st IEEE Conference on, pp. 641-648. IEEE, 2006.
26. Dunkels, A., Eriksson, J., Finne, N. and Tsiftes, N., 2011. Powertrace: Network-level power profiling for low-power wireless networks.

AUTHORS PROFILE

Dr.S.Prabavathy received the Ph.D. degree in Computer Science and Engineering from Anna University, India. Her research interests include Internet of Things, Fog Computing and Wireless network Security.

Dr.S.Prabavathy received the Ph.D. degree in Computer Science and Engineering from Anna University, India. Her research interests include Datamining and Wireless network