Hybrid Monitoring Technique for Detecting Abnormal Behaviour in RPL-Based Network

Mahmood Alzubaidi, Mohammed Anbar, Yung-Wey Chong, and Shadi Al-Sarawi
National Advanced IPv6 Center
Universiti Sains Malaysia, 11800 USM, Penang, Malaysia
Email: mahmood@nav6.usm.my; anbar@nav6.usm.my; chong@usm.my; shadi@nav6.usm.my

Abstract —Internet Protocol version 6 (IPv6) over Low Power Wireless Personal Area Networks (6LoWPAN) is extensively used in Wireless Sensor Networks (WSNs) due to its ability to transmit IPv6 packet with low bandwidth and limited resources. 6LoWPAN has several operations in each layer. Most existing security challenges are focused on the network layer, which is represented by its routing protocol for low- power and lossy network (RPL). The 6LoWPAN with its Routing Protocol (RPL) usually uses nodes that have constrained resources (memory, power, processor). In addition, RPL messages are exchanged among network nodes without using any message authentication mechanism. Therefore, the RPL exposes to various attacks that may lead to network disrupt. A sinkhole attack is one of the attacks that is utilizing the vulnerabilities in RPL and attract considerable traffic by advertising falsified information data that change the routing preference for other nodes. This paper intents to propose a hybrid monitoring technique for detecting abnormal behaviour in RPL -based network. The proposed technique is evaluated using Cooja simulator in term of power consumption and detection accuracy. Also, the proposed technique was compared with other popular detection mechanisms.

Index Terms—Internet of things, intrusion detection system, sinkhole attack, WSN, RPL, 6LoWPAN

I. Introduction

Wireless Sensor Networks (WSNs) have attracted a reasonable amount of research attention during last decade. Their limited resources and the hostile deployment environment put severe challenges to the research studies. As a result, the phenomena of the IOT (Internet of Things) is rapidly deploying and 50 billion small devices (or things) going to be linked to the Internet by 2020 [1]. So, the average is probably 6 devices for each person on the planet. Undoubtedly, a massive number of devices connected to each other as well to the internet which require high level of security and authentication because the exchangeable data traffic may contain critical information belongs to various fields such as home devices, medical devices, cars, flights as well nuclear reactors and other things, which may cost tangible risks to human life [2]. The existing traditional security mechanisms such as Intrusion Detection System (IDS), Firewalling, and Prevention Systems are deployed at an earlier stage of the Internet life are no longer sufficient to secure the next generation of the internet. Furthermore, the Wireless Sensor Networks architecture in the internet of things (IoT) provides additional interests and challenges over network security due to several reasons such as resource constraints, limited physical security, lack of infrastructure, unreliable links and dynamic topology. These characterises are particularly vulnerable and required more effort to protect them against insider or external attacks. Moreover, IoT devices are accessible from anywhere through untrusted network like the internet and therefore, cause IoT networks to be unprotected against a wide range of malicious attacks [3], [4]. Internet of Things (IoT) consists of smart devices that communicate with each other. It enables these devices to collect and exchange data. Besides that, IoT now have a wide range of life applications such as industry, transportation, logistics, healthcare, smart environment, as well as personal, social gaming robot, and city information. Smart devices can have wired or wireless connection. As far as the wireless IoT being the main concern, many different wireless communication technologies and protocols can be used to connect the smart device such as Internet Protocol Version 6 (IPv6), over Low Power Wireless Personal Area Networks (6LoWPAN) [5]. The 6LoWPAN network depends on an enormous number of distributed nodes, but however, it has many constraints such as processing capability, low battery life and radio range. Therefore, the 6LoWPAN implementation requires a desirable routing protocol that can efficiently overcome these constraints such as Routing Protocol for Low Power and Lossy Network (RPL) [5].

A. RPL

The Routing Protocol for Low-power and Lossy Network (RPL) is standardized in RFC4919 and RFC6550 [6], [7]. Low-power and Lossy Networks (LLN) have constraints on processing, memory, and energy. Therefore, typical routing protocol cannot be used. Because Low power and Lossy networks (LLN) links suffer from high loss rate, low data rate, instability, expensive bits, and dynamically formed topology. In addition, LLN covers both wireless and wired networks

Manuscript received January 22, 2018; revised May 4, 2018.
Corresponding authors: email: mahmood@nav6.usm.my
doi:10.12720/jcm.13.5.198-208

that require bidirectional links. The RPL topology based on Directed Acyclic Graph (DAG) is a directed graph with all the edges oriented in such a way that cycles do not exist, and the DAG root does not have an outgoing edge, thus failing to fulfill the need for WSNs. Therefore, destination-oriented DAG (DODAG) is deployed by introducing a single destination root, wherein up is toward the root, and down is away from the root. The position of each node in the DODAG graph is identified using the rank number, which clarifies the node distance from the root using a specified objective with respect to other neighbor nodes. The node in RPL network can join multiple DODAGs within the same RPL instance. DODAG ID is the IPv6 address of the root, and the DODAG version is the current version of the DODAG. Therefore, when a new DODAG is computed with the same root, its version increments. RPL has three main control messages. The first message is the DODAG information object (DIO), which multicasts downward in the RPL instance, and allows other nodes to discover the RPL instance and join it. The second message is the DODAG Information Solicitation (DIS), which is considered as the link-local multicast request for DIO neighbor discovery. The third message is the Destination Advertisement Object (DAO), which flows from the child toward the parents or the root, as presented above in Fig. 1.

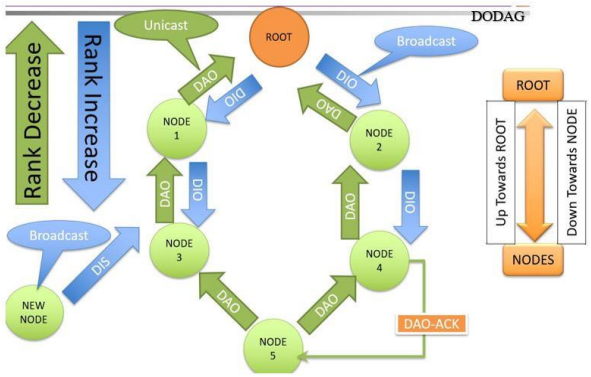


Fig. 1. Type of RPL message.

B. Security in RPL Network

The network layer in RPL provides security that protects the messages with confidentiality, integrity and availability services (CIA), although several attacks are possible against networks intent to break the CIA security paradigm. Intrusion Detection Systems (IDS) are required to detect malicious activities in the network. Furthermore, firewalls can block unauthorized access to networks from external attacks. In IoT, the limitation of 6LoWPAN network makes it vulnerable to several attacks from the Internet or internal network. RPL, a routing protocol for low-power and lossy networks is vulnerable to several routing attacks aimed to damage the topology. The IoT with 6LoWPAN networks running RPL as in Table I. shows the content of delicate security methods such as IP security (IPsec) and RPL security which are not sufficient against a certain network attack in WSN devices[6],[8], [7].

TABLE I: RPL SECURITY SOLUTION

IoT Layer	IoT Protocol	Security Protocol
Network Layer	IPv6, RPL	RPL Security
	6LoWPAN	IPsec

1) RPL default security

RPL offers various level of security defense by utilizing a security field in the 4-byte ICMPv6 message header. Information in this field defines the level of security which the cryptography algorithm should be used to encrypt the messages [6]. RPL can use its own three basic security modes. The first mode called as unsecured; meaning that RPL control messages are sent without any additional security mechanism except for the link-layer security. The second mode called pre-installed which rely on the pre-installed keys in RPL Instance nodes during the joining time to enable them to generate a message. Third security mode called authenticated which is an authentication key required from authority for joining an authenticated RPL Instance as host only or obtaining the second key in case if a node wants to join as a router. Those modes alone are not sufficient to protect RPL from attacks such as Sinkhole, Denial of Service attacks, Hello Flooding, Wormhole, Blackhole, Selective Forwarding or Sybil attack.

2) IPsec in RPL network

IPsec protocol is commonly used in IPv6 to establish end-to-end security for any IP communication, unlike 6LoWPAN which does not provide any model of security. Therefore, developer groups in RFC 4944 [9] and the research community in [10] consider IPsec as a potential security solution for the 6LoWPAN. However, IPsec is observed as a heavy weight security option for 6LoWPAN network, due to the limitation of the constrained nodes.

Raza *et al.* [10], [11] presented a lightweight 6LoWPAN/IPsec solution focusing on Encapsulating Security Payload (ESP) and Authentication Header (AH). Authors have used a compression mechanism to apply AH and ESP to a packet by introducing 6LoWPAN/IPsec extension compatible with the small header size in 6LoWPAN. AH gives data origin authentication, connectionless integrity and protection against replay attacks. Meanwhile, ESP gives origin authenticity, data integrity, and confidentiality protection. On the hand, even when confidentiality and integrity are applied by 6LoWPAN/IPsec solutions, several attacks against IoT devices have been successfully identified. However, those attacks against IoT are also possible to bypass IPsec solutions in IoT networks. Consequently, it is significant to have approaches technique that can detect the external and internal attacks [12], [13].

C. Sinkhole Attack in RPL Network

6LoWPAN network is possible to be source of attacks against Internet hosts, due to the high probability of

compromising a constrained node than a typical Internet host. According to Mayzaud *et al*. [14], IoT attacks are classified into three types based on the goal of the attacker and the final damages on the DODAG graph in RPL. The first category of attacks consumes the resource of the networks (energy, memory, and processing). The second category of attacks disrupts the topology of RPL, whereas the last category of attacks targets network traffic. This current review focuses on the attacks that have affected the topology of the DODAG graph in RPL, particularly the sinkhole attack that occurs in two steps as shown in Fig. 2. First, the malicious node can attract considerable traffic by advertising falsified information data for parent preference by the other nodes. Then, the malicious node may modify or drop it after receiving the traffic illegally.

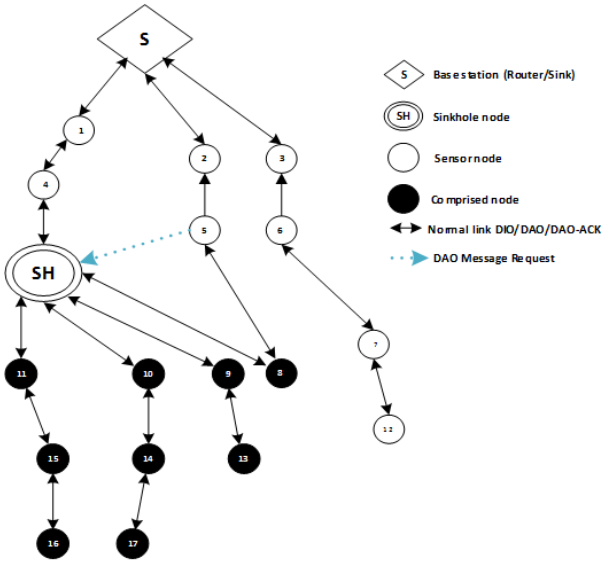


Fig. 2. Sinkhole node in RPL network.

In this paper, the proposed hybrid monitoring technique for detecting abnormal behaviour in RPL - based network is used to detect sinkhole attack that accrued due to the illegal decrement of node rank. The rank decreasing misleads as much network traffic as possible to one specific place. The malicious node which performs sinkhole attack is called sinkhole node. It usually claims itself as the shortest path to the base station (Sink) because of illegitimate rank decrement. Only one sinkhole node can attract surrounding nodes with falsified routing information. In addition, it is possible to execute serious malicious attacks such as the selective forwarding attack or altering the passing data because the sinkhole node can prevent the base station (Router) from obtaining complete and accurate data. The proposed technique is evaluated using Cooja simulator Eriksson *et al*. [15], Dunkels, Adam [16].

The main contributions of this paper are:

- Propose a hybrid monitoring technique for detecting abnormal behaviour in RPL -based network.
- Evaluate the proposed technique in term of power consumption and detection accuracy.
- Compare the proposed technique with other existing machinimas.

The rest of the paper is organized as follows. The next section briefly discusses the related work. Section 3 presents the proposed Technique. Section 4 discusses the result of the performance metrics and compares its performance with other exciting machinimas. Finally, Section 5 concludes the paper.

II. Related Works

The existing mechanisms used to detect sinkhole attacks in RPL can be categorized based on various aspects of RPL security [17], as illustrated in Fig. 3. Accordingly, this section provides a brief investigation covering related mechanisms.

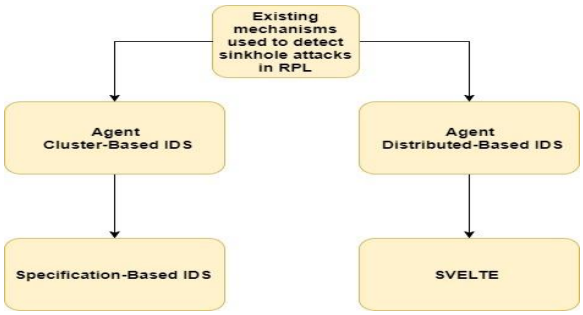


Fig. 3. Existing mechanisms for detection sinkhole attack in RPL.

A. Agent Distributed-Based IDS

Raza *et al*. [18], proposed an IDS called SVELTE which uses a hybrid of signature and anomaly-based detections with regard to balancing the storage costs of the signature-based detection and the computing cost of the anomaly-based techniques. Three main modules are placed in the root. The first module, called 6LoWPAN mapper, collects information regarding RPL and rebuilds the network in the root. The second module analyses the mapped data and detects intrusion. The third module, which is a distributed mini firewall, is designed to filter unwanted traffic before it enters the resource-constrained network, by contrast, the constrained node has two corresponding lightweight modules each. The first module provides mapping information to the root (6LoWPAN Border-Router) to detect intrusion, whereas the second module works with the centralized firewall. If the routing graph is inconsistent, then the node has a lower rank than its parent, indicating an occurrence of a sinkhole attack.

The agent distributed-based IDS, such as SVELTE [18], places an agent on both sides of the RPL. The first agent in the host node is for reporting, and the second agent in the DODAG root is for analyzing. These mechanisms have two drawbacks. First, the false positive detection due to the DODAG root has to report the information of the attacking node to each node. However, the information may pass through malicious nodes, which similarly perform as normal nodes; thus, the delivered information is ineffective. The second drawback is high

resource consumption due to the agent overhead processing, which is placed in each node.

B. Agent Cluster-Based IDS

The specification-based IDS is provided by Le et al. [19] to improve the SVELTE approach, such as providing low false positive rate and low resource consumption. The proposed specification IDS comprise two stages. First, the RPL using an extended finite-state machine to define all states that are related to the network topology stability and analyse those transition states by using a trace file. The second stage translates the knowledge of the RPL profile using detection algorithms that are placed in the IDS agent. The hybrid or clustering architecture has advantages compared to other approaches such as SVELTE. Furthermore, the IDS agent is cluster-based, which is placed in each cluster head and records the relevant information from its members. There is a low resource consumption because of the lack of overhead processing on each node, while the cluster head can obtain more resources to deal with the IDS work. The specification cluster approach solves the synchronization issue that causes the high false positive during the message exchange between the nodes in the previous approach by adding the sequence number information in the DIO and DIS messages. The reserved bytes in the DIO and DIS message format is used; thus, the sequence number where the packets of information belong are specifically defined, and the agent can cross-check only the sources that have the same sequence.

Agent cluster-based IDS proposed by Le *et al*. [19] adopted SVELTE and overcame its problems by proposing cluster-based IDS. However, the cluster-based IDS can fail due to centralization. Furthermore, when the IDS agent in the cluster head goes down due to power or attack, the IDS will no longer be functional.

The following Table II. provides a comparison of those mechanisms.

TABLE II: SUMMARY OF MECHANISMS USED TO DETECT SINKHOLE ATTACK ON RPL.

Mechanisms	Countermeasure method	Drawbacks
SVELTE	IDS agent placed in the host node and the main root	High false positive, resource consumption
Specification cluster-based	Cluster-based IDS centralizes the agent in the middle of the node graph to reduce the overhead on the nodes and the root	Improve the resource consumption issue and the false positive issue in SVELTE however, it introduces a high probability of IDS failure due to centralization

III. PROPOSED HYBRID TECHNIQUE

Before introducing the details of the proposed hybrid technique, we first give some definition for related terms.

- **The passive intermediate node (PN1):** is a sensor that has sufficient resources and high radio range to gather data and close to the network sink.
- **The passive edge node (PN2):** is a sensor that has sufficient resources and high radio range to gather data and not close to the network sink range.
- **The passive nodes**: all passive nodes that are a listener and communicate with each including the sink to ensure there is no wastage of the network power.

There are two possible assumptions in terms of how the suspicious/sinkhole node is close to the passive nodes. Fig. 4. Shows how the passive nodes are placed in RPL network.

The first assumption that suspicious/sinkhole node could be located beside the base station (router/sink) which covered by the passive intermediate node (PN1). As illustrated in Fig. 4 which contains five nodes (D, G, F, I, H) that close to the base station and inside the range of PN1.

The second assumption that suspicious/sinkhole node could be located far from the base station (router/sink) which inside the range of the passive edge node (PN2). in Fig. 4 there are four nodes (A, B, C, E) is far from the sink and the passive intermediate node (PN1) but covered within the range of passive edge node (PN2).

A. Overview of Proposed Hybrid Technique

The hybrid technique contains the following two main phases:

1. Identifying suspicious nodes: each passive node collects neighbour nodes data and analyse it to identify suspicious based on node rank. As shown in Fig. 4.
2. Detect sinkhole nodes: by compared the data from the two passive nodes to detect the sinkhole nodes from suspicious nodes based on node ID.

1) Identifying suspicious nodes

In RPL DODAG, each node broadcast DIO message via multi-hop routing starting from the base station (router/Sink) toward the bottom of the RPL tree. Thus, the passive node with sufficient resource and high radio range is placed in the middle of a group of nodes and able to receive all neighbour nodes broadcast. After the passive node collects data such as node ID and rank, the passive node starts examining neighbour nodes based on their rank. On another word, all neighbour nodes should carry similar rank value. But when the neighbour node has lower rank value compared to its neighbour node, then the passive node will identify that node as a suspicious node and move to detection phase.

The passive intermediate node (PN1) as shown in Fig. 4 is listening to the broadcast for nodes in a passive mode such as nodes D, F, G, H and I. Passive intermediate node will check the captured data and analyse it for all nodes. If the nodes are a neighbour and carrying similar rank, there is no suspicious node is detected. But if nodes are a

neighbour but their rank is totally different, then there is suspicious node is detected.

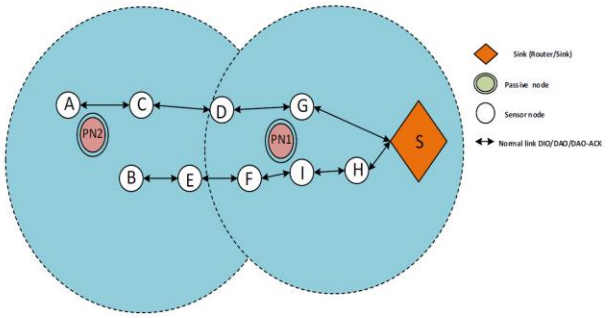


Fig. 4. Two types of passive nodes

The passive edge node (PN2) is not close to the sink node but within the range PN1. For each time the passive edge node (PN2) as shown in Fig. 4 listens to the nodes broadcasting in a passive mode such as nodes A, B, C and E. Passive edge node will check the collected data and analyse it. If nodes are neighbour and carrying similar rank, there is no suspicious node is detected. But if the nodes are neighbour of each other but carrying different rank, there is suspicious node detected.

Suspicious node detected based on the two conditions as below:

Case 1: If the passive edge node table contains a node that does not carry similar rank to another node, thus, there is a suspicious node in the area of PN2. For example, in Fig. 4 if node C is carrying totally different rank compared to nodes A, B and E, so it can be concluded that C is a suspicious node.

Case 2: If the passive intermediate node table contains a node that does not carry similar rank to another node, thus, there is a suspicious node in the area of PN1. For example, in Fig. 4 if node I, is carrying totally different rank compared to nodes D, F, G and H, so it can be concluded that I is a suspicious node.

2) Detection sinkhole nodes

The second phase is detection sinkhole nodes which come after the first phase which is identifying suspicious nodes, as clarified in the previous section. In addition, in the detection phase, the sinkhole node must be detected among the suspicious nodes. The general idea is to detect and differentiate the suspicious nodes one by one. Therefore, this phase of detection sinkhole nodes contains the following two stages:

Stage 1: The passive edge node (PN2) send a query packet to the passive intermediate node (PN1), about the suspicious node that has a lower rank and claimed to be closer to the sink, let assume it is C node as shown in Fig. 4 Then, after receiving the neighbor query packet, the passive intermediate node (PN1) immediately replies to the edge passive node (PN2).

Stage 2: Based on the reply packets from the first passive intermediate node (PN1), the passive edge node (PN2) checks where Node C ID exists in PN1 Table. So, if the node C ID exists in the PN1 table, then it's true that the node C with the lower rank node is close to the sink area and no sinkhole node is detected. On other hand, if the node C ID does not exist in the PN1 table, then node C has falsely lower rank and detected as a sinkhole node.

B. Network Modelling

This section, explain in detail the steps of the experiment and dataset collection based on the different scenario. The first step is to construct RPL DODAG topology and set the parameter as provided in Table III. then running the simulator for the basic DODAG topology without any attack for a specific time and collect two types of dataset. The first dataset is packet analyser and network layer message which is collected using 6LoWPAN analyser in Cooja simulator. The second dataset is power consumption of each sky mote, the powertracer tool has been used to calculate the power consumption. In The second step, the same producers are repeated with and without the proposed technique. The proposed technique is evaluated on three different scenarios. The first scenario with one sinkhole attack is placed in the network, the second scenario with two sinkhole attacks are placed in the network, the last scenario where three sinkhole attacks are placed. The performance metrics, power consumption, and detection accuracy are evaluated in Section 4.

TABLE III: PARAMETER SETTINGS OF THE RUNNING SIMULATION

Parameters	Values
Mote type	skymote
Network window size	200 ×200 ^{m2}
Routing protocol	RPL
Running time	5 minutes
Simulating speed	100 %
Total Number of nodes including sink	20
Topology design	Tree
Power monitor runtime	10 second
Sink node ID	1
Passive nodes ID	21,22
Attack Node ID	2

C. Power Consumption Modelling

To calculate power consumption in Cooja simulator, the dataset that generated from powertracer tool is used. The Powertracer tool is included in the Makefile as following:

APPS += powertrace

In the programme of both nodes unicast-reciver.c and unicast-sender.c, the following lines of code are included to print out 8 different values of each node for power consumption.

#include "powertrace.h"

powertrace_start (CLOCK_SECOND * 10); for example, in the mote when the Runtime value is 10 this means that the values for power consumption will be printed every 10 seconds. Table IV shows fields that mote outputs while using powertracer tool.

TABLE IV: THE OUTPUT VALUES USING POWERTRACE

1	2	3	4
clock_time()	P	rimeaddr_node_addr.u8[0], rimeaddr_node_addr.u8[1]	seqno
5	**6**	**7**	**8**
seqno	all_cpu	all_lpm	all_transmit

The above Table IV shows several states of values for the Sky mote as a number of clock ticks. Field number 5 all_cpu is the total (high) CPU (CPU in active mode). While field number 6 all_lpm is the total number of ticks in a state LPM (Low power mode). Also, field number 7 all_tx is representing the total number of ticks in tx (Transmit), finally field number 8 all_rx is the number of ticks in the Rx (Receive). The power consumption is calculated using the following formulas [20], [21]:

$$\text{Energy (mJ)} = \frac{\text{Energest}_{\text{Value}} * \text{Current} * \text{Voltage}}{\text{RTIMER}_{\text{SECOND}}}$$

$$\text{Power Consumption } (mW) = \frac{Energy\ (mJ)}{Time(s)}$$

In this experiment, the skymote node has been used as receiver and sender node in our simulator. Therefore, RTIMER_SECOND is 32768, the voltage for Sky mote is 3V and the current values for Skymote is fixed. As shown in the Sky mote Table V, [22].

TABLE V: SKY MOTE CONDITION

Conditions	Normal	Unit
Voltage	3	V
Listen RX	21.8	mA
Transmit TX	19.5	mA
CPU	1.8	mA
LPM (Low Power Mode)	0.0545	mA

D. Detection Accuracy Calculation

The detection Rate is to shows how the hybrid technique is accurate in detecting the sinkhole node. Therefore, each scenario has been repeated for ten times to calculate the true positive (TP), false positive (FP) and the detection accuracy rate. The formula to calculate these three metrics are:

$$True\ Positive\ Rate\ (TPR) : = \frac{TP}{TP + FN}$$

$$False\ Positive\ Rate\ (FPR) : = \frac{FP}{FP + TN}$$

$$Detection\ Accuracy\ \ Rate : = \frac{TP + TN}{(TP + TN + FP + FN)}$$

IV. PERFORMANCE OF HYBRID TECHNIQUE

Hybrid technique is evaluated in terms of two performance metrics, the power consumption and detection accuracy to determine the overall improvement. Furthermore, hybrid technique performance is compared with most popular cluster and distributed mechanisms for detection sinkhole attack in RPL network [18], [19].

A. Evaluation of Power Consumption

Power consumption is calculated separately for each consumption source in the micro-computer unit (MCU) of skymote node. As described in Table 6. The total power consumption is calculated for consumption sources in a node.

TABLE VI: POWER CONSUMPTION SOURCES IN SKYMOTE NODE

Consumption source	Description
CPU	micro-computer unit (MCU) is on and the radio is off
LPM	MCU is idle while the radio is off
RX	the radio is receiving while MCU is on
TX	the radio is transmitting while MCU is on

The experiment time for power consumption is five minutes for each scenario. Five minutes without the proposed hybrid technique and five minutes with the proposed technique. In all scenarios, the changes of power consumption for the sink, the attacker node, and the whole network have been monitored during each experiment.

1) The power consumption of the sink node

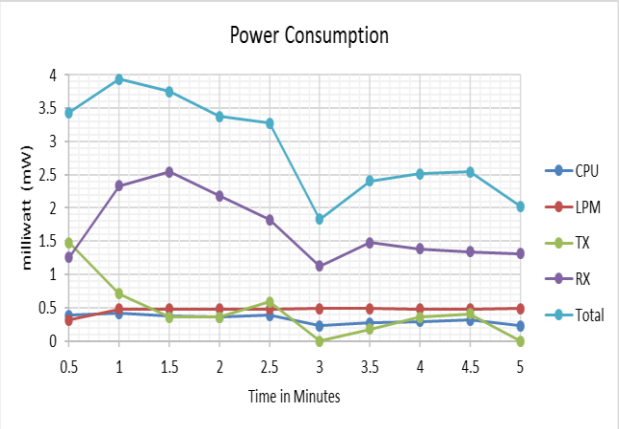


Fig. 5. Power consumption of sink node in one attack scenario with proposed technique.

The changes that happen to the power of the sink node with the proposed technique and without is totally different compared to another node. Furthermore, the power consumption of the CPU, LPM, and TX are almost same with the proposed technique and without as shown

in Fig. 5 and Fig. 6. However, the RX in sink node with proposed technique consumes more power 4 milliwatts (mW) than RX without proposed technique. this because the sink back to normal and starts receiving legitimate RX traffic, where without proposed technique the traffic that sends to the sink node was obtained by other compromised nodes, so the power consumption of RX is reduced in the sink.

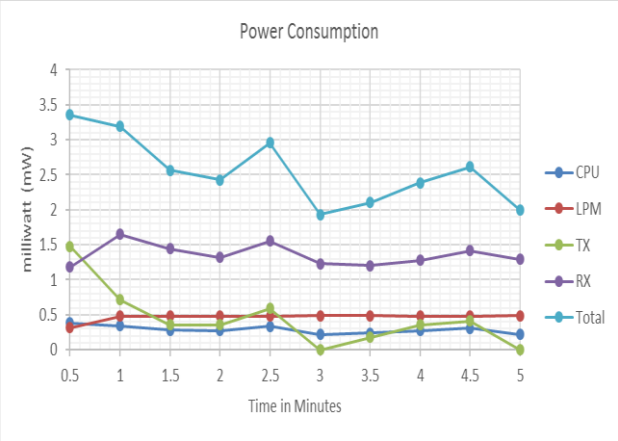


Fig. 6. Power consumption of sink node in one attack scenario without proposed technique.

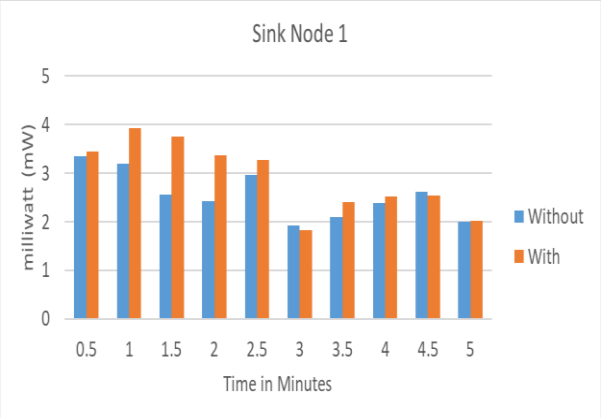


Fig. 7. Total Power consumption for sink node in first scenario with proposed technique and without.

Fig. 7 shows the total power consumption with and without the proposed technique, sink node with hybrid technique in 5 minutes consumed 29 (mW) while without proposed technique 25 (mW). Furthermore, with proposed technique the network receives the entire legitimate traffic, so the sink node must consume power due to RX processing, but when there is compromised node in the network the RX processing in the sink node goes down due to traffic lose So as a conclusion, the proposed technique detects the sinkhole attack without power wastage and the sink node is back to the ideal operation mode, in particular, receiving all legitimate RX traffic without any loss.

2) The power consumption of the sinkhole node

The changes that happen to the power of the sinkhole node (Attacker) with the proposed technique and without is totally different compared to changes that happen with the sink node. Furthermore, the power consumption of the CPU, LPM, TX, and RX without proposed technique is highly increased compared to the power that consumed with proposed technique. The power consumption of the sinkhole node with proposed technique and without is shown in Fig. 8 and Fig. 9. However, the power consumption of the CPU in sinkhole node without proposed technique consumes power 15 milliwatt (mW) more than with proposed technique. This wastage of power due to the high processing of the illegitimate traffic in the Sinkhole node. The sinkhole node is processing two type illegitimate traffic, the received traffic RX and the transmitted traffic TX.

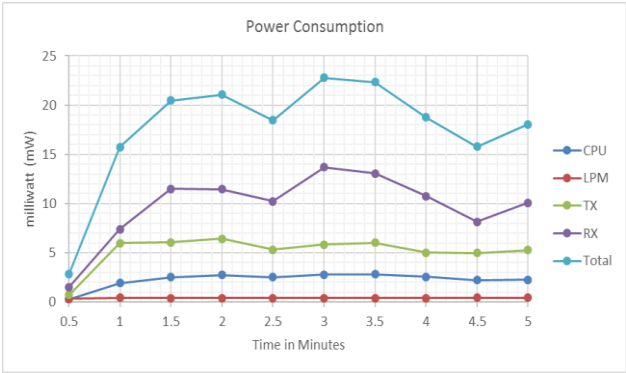


Fig. 8. Power consumption of attacker node in one attack scenario without proposed technique.

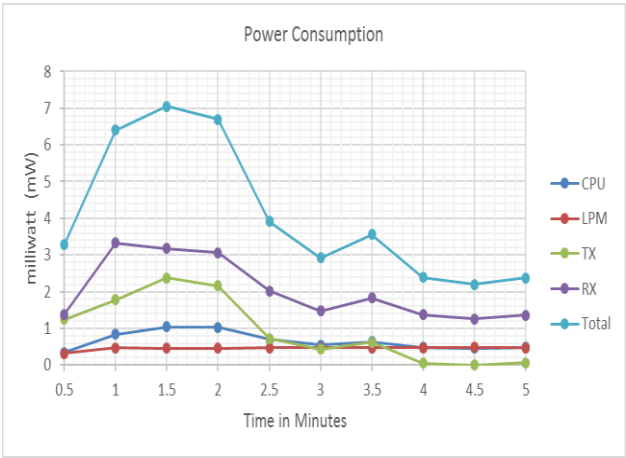


Fig. 9. Power consumption of attacker node in one attack scenario with proposed technique.

When the sinkhole node decreases its rank, it attracts more illegitimate traffic from other nodes. The power consumption of RX without proposed technique is increased to 77(mW) due to receiving illegitimate DAO and DIS messages. Likewise, the power consumption of TX without proposed technique is increased to 41(mW) due to transmitted illegitimate DIO messages. Fig. 10 shows the total power consumption with and without the proposed technique, the sinkhole node with proposed technique in 5 minutes consumed 40 (mW) while without proposed technique 170 (mW), so as a conclusion, the proposed technique works as lightweight detection technique without effect or causing any wastage of the whole network power.

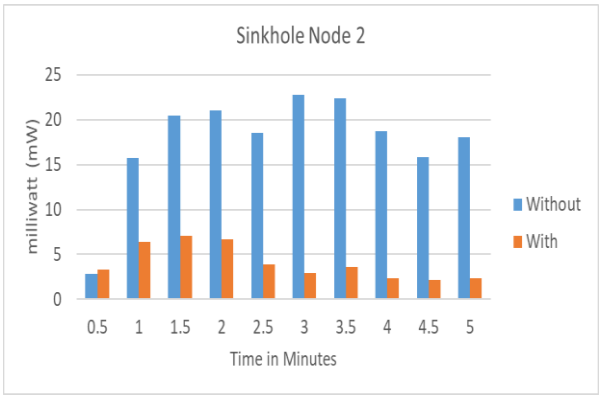


Fig. 10. Total power consumption for the attacker node in one attack scenario with proposed technique and without.

3) The power consumption of the whole network

This section highlights the power consumption with proposed technique and without for the whole network that contains 20 nodes. Overall the power consumption of the CPU, TX, and RX without proposed technique is highly increased compared to the power that consumed with proposed technique. The power consumption of the whole network with proposed technique and without is shown in Fig. 11 and Fig. 12. However, the CPU for all nodes without PNMT consumes more power 58 milliwatts (mW) than CPU with proposed technique in all nodes. This wastage of power due to the high processing of the illegitimate traffic in the whole network nodes. So, without the proposed technique, the sinkhole node is processing two type illegitimate traffic, the received traffic RX and the transmitted traffic TX. In addition, without proposed technique the power consumption is increased not only in the sinkhole node, but in the whole network nodes, including the power of CPU, RX, and TX.

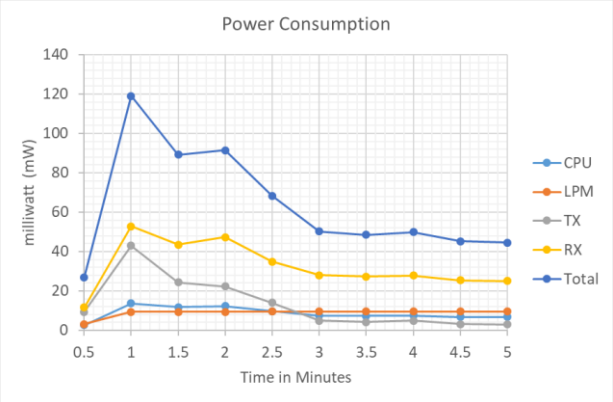


Fig. 11. Power consumption of attacker node in first scenario with proposed technique.

The sinkhole node increases the power consumption for all network, due to the inconsistent flow of the whole network messages. The power consumption of RX without proposed technique for the whole nodes is increased to 461 mW due to receiving illegitimate DAO and DIS messages. Likewise, the power consumption of TX without proposed technique is increased to 184 mW due to transmitted illegitimate DIO messages. Fig. 13 shows comparison of power consumption with and without the proposed technique, the whole network nodes with proposed technique in 5 minutes consumed 633 mW while without 1200 mW, so as a conclusion, the proposed technique works as lightweight detection technique without effect or causing any minimal power wastage on the node battery.

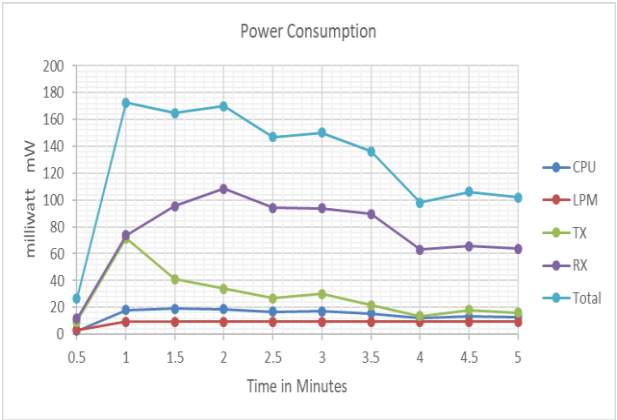


Fig. 12. Power consumption of attacker node in first scenario without proposed technique.

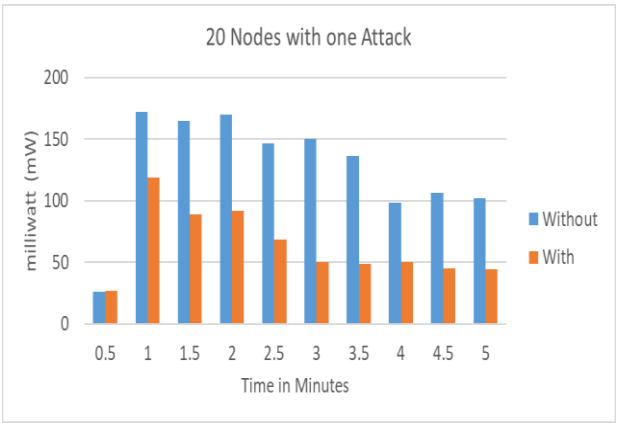


Fig. 13. Power consumption of networks nodes in one attack scenario with and without proposed technique.

B. Evaluation of Detection Accuracy

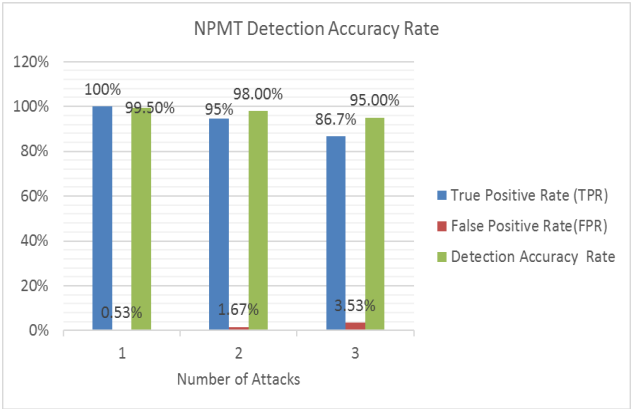


Fig. 14. Detection accuracy of proposed technique based on three scenarios.

The true positive rate and false positive rate for the first scenario is presented in Table VII. The first scenario is repeated ten times which include only one sinkhole

node, each time is five minutes. The result shows that the true positive rate is 100% that means the sinkhole node is detected in each experiment by the proposed technique. However, the false positive rate is 0.53% because in the experiment number 8 the proposed technique detects one legitimate node as a sinkhole node. The false detection error happens because one of the sinkhole child nodes decreased its rank which not within the rank that fixed earlier by the passive node. Overall, the average detection accuracy in one attack scenario is 99.50% which proves the efficiency of the proposed technique. The overall detection accuracy in all scenarios is presented in Fig. 14.

TABLE VII: TRUE POSITIVE AND FALSE POSITIVE IN ONE ATTACK SCENARIO

Number of experiment	True Positive (TP)	False Positive (FP)	Detection Accuracy
1	1	0	1
2	1	0	1
3	1	0	1
4	1	0	1
5	1	0	1
6	1	0	1
7	1	0	1
8	1	1	0.95
9	1	0	1
10	1	0	1
Average TP/FP / Detection Accuracy Rate	100%	0.53%	99.50%

C. Comparative Study for Proposed Technique

This section compares between proposed technique and other two existing detection mechanisms in term of power consumption and detection accuracy. First mechanism is SVELTE proposed by Raza *et al*. [18] and second mechanism is specification-based IDS proposed by Le *et al*. [19].

1) Power consumption comparative

Table VIII below is provided by Raza *et al*. [18] to show the overhead of the placing SVELTE IDS on each node in mJ. So, we calculate the result in mJ and divided on our running time (5 minutes) to get the power consumption in mW.

TABLE VIII: ENERGY CONSUMPTION FOR HANDLING A SINGLE EVENT INSIDE A CONSTRAINED NODE [16]

Event	Energy (mJ)
6Mapper response handling	0.1465
Firewall handling	0.0478
Packet lost correction	0.0483

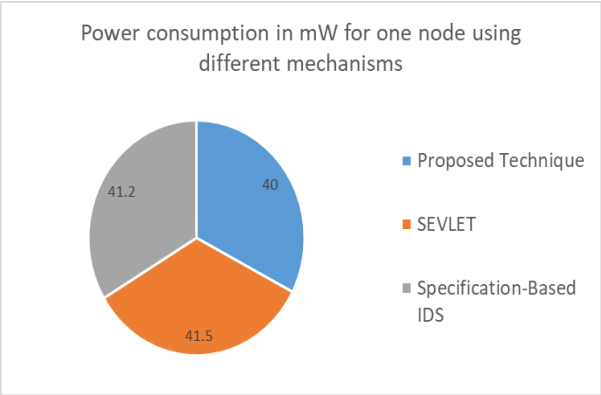


Fig. 15. Average power consumption of each node in different mechanism.

In the specification-based IDS Le *et al*. [19] mentioned that, the power consumption in the proposed IDS is 1.2 mW for each node. Fig. 15 shows that the proposed technique is less power consumption and save the battery life of the node compared to SEVLET and Specification-Based IDS.

2) Detection Accuracy comparative

This section only compares the true positive rate between the proposed technique, SEVLET and Specification-Based IDS. Table IX shows the true positive rate are similar in the proposed technique and Specification-Based IDS, while SEVLET has lower true positive rate.

TABLE IX: TRUE POSITIVE RATE FOR DIFFERENT MECHANISMS

Mechanism	True Positive Rate (TPR)
Proposed Technique	100%
Specification-Based IDS	100%
SEVLET	90%

V. CONCLUSION

The main idea of this paper comes from the need of protecting the constrained RPL network against internal attacks based on lightweight technique. Therefore, a hybrid monitoring technique for detecting abnormal behaviour in RPL -based network is proposed. The proposed technique is designed to meet the requirement of the constrained nodes without causing power overhead and save node energy. Usually distributed detection mechanisms such as SVELTE is caused heavy processing inside each node, which leads to high power consumption and shortage the battery life of the constrained node. In this research, the passive node has been introduced with sufficient resource, so the passive node can handle data processing and analysis without affecting the rest of network constrained nodes. The power consumption and detection accuracy are two performance metrics that evaluated. The result shows, that with the proposed technique power consumption of each node is reduced to 55%. Also, detection accuracy rate of the proposed

technique is over 90% as average of all experiments. In addition, comparative result shows that, with the proposed technique is much efficient than SVELTE and specification-Based IDS in term of power consumption as well the detection accuracy.

As for future work, the proposed technique can be extended to detect other protocols anomalies, Also, the can be combined with other signature-based Introduction Detection System (IDS). The collected dataset has a limited number of nodes and attacks. Thus, as for future work, the result can be quite different based on to the different datasets and scenarios.

The mitigation phase can be added as an extended future work in this research. the attack mitigation can be achieved via two possible phases. First phase includes the following steps: (i) When the sinkhole node is detected, passive node turns to active mode and sends rank-repair command to the sinkhole node. (ii) Sinkhole node received command and starts auto rank-repair, in the meanwhile the passive node keep monitoring. Second possible mitigation phase includes the following steps: (i) When the sinkhole node is detected, passive node sends sinkhole node details to the main root. (ii) Root received passive node update regarding sinkhole node, root sends broadcast DIO message to update the network version and exclude the sinkhole ID to be chosen as parent node.

ACKNOWLEDGMENT

The research project is funded by Digi Telecommunications Sdn Bhd under grant number 304/PNAV/650764/D113.

REFRENCES

[1] V. Adat and B. B. Gupta, "Security in internet of things: Issues, challenges, taxonomy, and architecture," *Telecommunication Systems*, 2017.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] T. Sherasiya, H. Upadhyay, and H. B. Patel, "A survey: Intrusion detection system for internet of things," *International Journal of Computer Science and Engineering*, vol. 5, no. 2, 2016.

[4] T. Zhang and X. Li, "Evaluating and analyzing the performance of rpl in contiki," in *Proc. First International Workshop on Mobile Sensing, Computing and Communication*, 2014, pp. 19–24.

[5] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, "Internet of Things (IoT) communication protocols," in *Proc. 8th International Conference on Information Technology*, 2017, pp. 685–690.

[6] P. Thubert, C. Bormann, L. Toutain, and R. Cragie. (2017). IPv6 over low-power wireless personal area network (6LoWPAN) Routing Header. [Online]. (8138). Available: http://www.rfc-editor.org/info/rfc8138

[7] R. Alexander, A. Brandt, J. Vasseur, J. Hui, *et al*., "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," *Internet Requests for Comment*, no. 6550, 2012.

[8] N. Kushalnagar, G. Montenegro, C. Schumacher, and others, "IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals," *RFC4919*, vol. 10, August 2007.

[9] G. Montenegro, J. Hui, D. Culler, and N. Kushalnagar, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," in *Proc. International Conference on Signal Processing & Communication Systems*, 2007.

[10] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig, "Securing communication in 6LoWPAN with compressed IPsec," in *Proc. International Conference on Distributed Computing in Sensor Systems and Workshops*, 2011, pp. 1–8.

[11] S. Raza, S. Duquennoy, J. Höglund, U. Roedig, and T. Voigt, "Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN," *Security and Communication Networks*, vol. 7, no. 12, pp. 2654–2668, 2014.

[12] L. Wallgren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL-based Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013.

[13] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6LoWPAN: A study on QoS security threats and countermeasures using intrusion detection system approach," *International Journal of Communication Systems*, vol. 25, no. 9, pp. 1189–1212, 2012.

[14] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Schönwälder, "Using the RPL protocol for supporting passive monitoring in the internet of things," in *Proc. Network Operations and Management Symposium*, 2016, pp. 366–374.

[15] J. Eriksson, F. Österlind, N. Finne, N. Tsiftes, A. Dunkels, T. Voigt, R. Sauter, and P. J. Marrón, "COOJA/MSPSim: interoperability testing for wireless sensor networks," in *Proc. 2nd International Conference on Simulation Tools and Techniques*, 2009, p. 27.

[16] A. Dunkels. (2008). Contiki Crash Course. Wireless sensor network programming: An introductio. Swedish Institute of Computer Science. [Online]. Available: http://www.ee.kth.se/\~mikaelj/wsn_course.shtml

[17] M. Alzubaidi, M. Anbar, S. Al-Saleem, S. Al-Sarawi, and K. Alieyan, "Review on mechanisms for detecting sinkhole attacks on RPLs," in Proc. *8th International Conference on Information Technology*, 2017, pp. 369–374.

[18] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the internet of things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

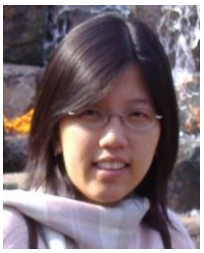
[19] A. Le, J. Loo, K. K. Chai, and M. Aiash, "A specification-based IDS for detecting attacks on RPL-based network topology," *Information*, vol. 7, no. 2, p. 25, 2016.

[20] P. Pongle and G. Chavan, "Real time intrusion and wormhole attack detection in internet of things," *International Journal of Computer Applications*, vol. 121, no. 9, 2015.

[21] A. Velinov and A. Mileva, "Running and testing applications for contiki OS using cooja simulator," in *Proc. International Conference on Information Technology and Development of Education*, 2016.
[22] T. Sky, "Ultra low power IEEE 802.15. 4 compliant wireless sensor module," *Moteiv Corporation*, 2006.

Mahmood Alzubaidi obtained his BSc degree from University of Greenwich, UK in 2016. He is currently a Master candidate in National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His interested research areas are Internet of Things (IoT), 6LoWPAN security, ad-hoc, sensor network, and intrusion detection system.

Mohammed Anbar obtained his PhD in Advanced Computer Networks from University Sains Malaysia (USM). He is currently a senior lecturer at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include Malware Detection, Web Security, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Network Monitoring, Internet of Things (IoT), and IPv6 Security.



Yung-Wey Chong is a lecturer at National Advanced IPv6 Centre of Excellence, Universiti Sains Malaysia with prior experience in telecommunication industry. She joined the center in 2009 as a research staff member, working in wireless communications. She is a committee member of SOI Asia (www.soi.asia), a project that utilizes satellite based Internet to support interactive multimedia communications between partner universities. She is also involved in CONNECT2SEA project (www.connect2sea.eu), a project funded under FP7, that support European Union and South-East Asia ICT strategic partnership and policy dialogue. At national level, she is an active member of MYREN and Connected Healthcare Cluster hosted by CREST. Her research interests are wireless communication, Internet of Things (IoT) and software defined networking.

Shadi Al-Sarawi obtained his MSc degree from Arab Academy for Banking and Financial Sciences, Jordan in 2004. He is currently a PhD candidate in National Advanced IPv6 Center (NAv6). *Universiti Sains Malaysia*. His interested research area are Intrusion Detection System(IDS), 6LoPAN, Internet of Things(IoT) Attacks, and Routing Protocol for Low-Power and Lossy Networks (*RPL*) security.