International Journal on Emerging Technologies **10**(2): 462-466(2019)

ISSN No. [Print] : 0975-8364
ISSN No. [Online] : 2249-3255

Specification Based Intrusion Detection Mechanism for Mitigating Sinkhole Attack in Wireless Sensor Networks

***Ranjeeth Kumar Sundararajan*[1]*, Narendran, S.M.*[2] *and Umamakeswari, A.*[2]**
[1]*Srinivasa Ramanujan Centre, SASTRA Deemed to be University, Kumbakonam, India.*
[2]*School of Computing, SASTRA Deemed to be University, Thanjavur, India.*

(Corresponding author: Ranjeeth Kumar Sundararajan)

(Received 01 June 2019, Revised 02 August 2019 Accepted 19 August 2019)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Wireless Sensor Networks is a resource constrained ad hoc network deployed in a hostile environment. This kind of network faces many security issues and security mechanisms plays a major role in it. Acknowledgement based security schemes is one of the important method used to counter the security threats in the sensor network. Sink hole is one of the most dangerous network layer threat to the network. This attack uses the routing metric as a vulnerable way to capture a node and drops the entire packets, which leads to greater network degradation and threat to the software systems of the network. Intrusion Detection System is one of the efficient security mechanisms to counter the routing attacks by raising alarms and alerting the network. This paper proposes a generic specification based intrusion detection model namely SEAACK to counter the sinkhole attack. This scheme apply the specification based algorithm to confirm the presence of sinkhole nodes. The proposed SEAACK mechanism is simulated in NS2 and the results show that SEAACK out performs the well-known existing schemes like Enhanced Adaptive Acknowledgement scheme (EAACK) in terms of QoS metrics like packet drop ratio, packet delivery ratio, normalized overhead and throughput etc.

Keywords: Wireless Sensor Networks, ACK, TWOACK, AACK, Sinkhole attack, Intrusion Detection System

I. INTRODUCTION

Wireless Sensor Networks (WSN) is placed in hostile environment in which the security is the major concern. WSN has variety of applications like military surveillance, environmental monitoring, computer science, and electronics and soon. WSN is anad-hoc network that is deployed in remote environments. Because of its nature of deployment, the sensor network is vulnerable to many security threats. The threats can bein many forms, either from insider or outsider of the network. The attacks can be classified based on protocol layer, location of the attacker, mode of operation and soon. The threats can be classified based on the WSN protocol stack. Depends on the location, the attacker may be classified into insider attacker or outsider attacker. Based on the mode of operation, the intrusion can be classified into active attack and passive attack. The active attack involves in altering the data, while passive attack involves only overhearing the communication between two entities.

There are many security mechanisms that exists in the literature for WSN. These mechanisms can be classified in to low- level and high-level mechanisms. The low-level schemes are Key establishment, Cryptographic schemes and Secure aggregation, Intrusion Detection Systems (IDS) are classified as the high-level security mechanisms [1]. The IDS is believed to be the second level of defense to protect the network. The IDS is generally classified into three types, Signature-based, Anomaly-based and Specification-based methods [10]. The signature based scheme contains the well-known attack patterns, and the observed traffic is matched with the known patterns or signatures. If, the pattern matches the observed traffic, then the IDS triggers the alarm. Signature based method is also known as knowledge based detection. The anomaly based scheme contains the legitimate behavior patterns and if, the observed traffic differs from the normal pattern, then the IDS triggers the alarm.

Anomaly method is also known as behavior based detection. The specification based scheme contains the manually developed specification of legitimate behaviors, which identifies the normal pattern, if the observed traffic deviates from the specifications, then the IDS alarms the network.

Table 1: Layer-Wise Threats.

Layer	**Threats**
Physical	Jamming, Tampering
DataLink	Collision, Exhaustion, Unfairness
Network	Sinkhole, Wormhole, Selective forwarding
Transport	Flooding, False Messages, De-synchronization
Application	Reliability attack, Clock Skewing, Data aggregation distortion

Specification based method is also known as stateful protocol analysis [3]. WSN needs a light weight mechanisms to counter the routing attacks [8]. This paper proposes a light weight generic specification based IDS to counter the network layer threat namely sinkhole attack in the acknowledgement based routing environment.

The paper is organized as follows: Section II gives the recent works in the literature, Section III brief the research background, Section IV gives the proposed work, Section V discusses the results and Section VI concludes the paper with the future work.

II. LITERATURE SURVEY

Djamel Djenouri [11] introduces the five different modules to identify the misbehaving nodes. The modules are monitor, detector, isolator, investigator and witness. The monitor module control the forwarding of packets, detector module detects the misbehaving of monitor nodes, isolator isolates the detected misbehaving nodes, and investigator investigates the accusing nodes and witness module respond to the witness request of the isolator. This method increases the computational overhead due to several splitting of the detection process. Elahdi [5] proposed enhanced adaptive scheme which consists of several steps to identify the malicious nodes like ACK, S-ACK and MRA. This scheme requires to find new route to communicate to the destination node to confirm the correctness of the malicious report, which increases the computation. TWOACK scheme is introduced by Liu *et al.* [2] to resolve two of the weakness of the watchdog scheme [7] namely receiver collision and limited transmission power. This scheme requires every three consecutive nodes to participate in the process. Upon receiving the packet, the node which is two hop away from it down the route is required to send the acknowledgement packet within predefined time, otherwise the nodes are declared as malicious nodes. This process increases the communication overhead and limited battery power degrade the lifetime of the network. AACK scheme is introduced by Sheltami *et al.* [4] to reduce the overhead of the acknowledgement transferred. The source node send the packet with 2b of flag indicating the packet type. The destination node after receiving the packet send back the acknowledgement in the reverse route to the source node. If, the acknowledgement packet is not sent to the source within predefine time, then it switches to TACK (Two Acknowledgement scheme). This process also suffer from the issue and fail to detect the malicious nodes in the presence of false misbehavior report and fake acknowledgement packets.

III. RESEARCH BACKGROUND

A. Acknowledgement Schemes

The Acknowledgement based IDS is also one of the important method to detect the intrusion in wireless sensor networks which is a resource limited environment. There are few existing acknowledgement based schemes in the literature like TWOACK [2], AACK [4] and EAACK [5]. These schemes requires that the destination node need to acknowledge the request of the source within some predefined period of time, if not then they come to a conclusion that there may be some malicious activity. The existing scheme EAACK scheme is taken as the well-known acknowledgement scheme for comparative study.

EAACK scheme: The Enhanced AACK scheme is introduced by Elhadi et al. [5] to solve the three weakness of the watchdog scheme [7]. This existing scheme has three parts, ACK, S-ACK, and MRA.

ACK: This is an end-to-end acknowledgement scheme, in which the source node send the ACK data packet to the destination node. When all the intermediate nodes are normal, the destination node reply with ACK packet along the reverse route to the source. If the ACK packet doesn't reach the source within certain period of time, then it switches to S-ACK step.

S-ACK: This step is an improved version of TWOACK method, in which the three consecutive nodes work in a group to detect misbehaving nodes in the network. If, the intermediate nodes doesn't send the ACK packet to the source within predefined time, then a misbehavior report is sent to source indicating the presence of malicious nodes. The control switch to MRA mode to confirm the correctness of the misbehavior report.

MRA: Misbehavior Report Authentication (MRA) authenticate whether the destination node had received the packet. The source node seeks an alternate route to the destination node, if there is no route, then DSR route request process is initiated to find another route. When the destination node receives the reported packet, then the misbehavior report is false otherwise, the report is true.

This scheme requires all the acknowledgement packets to be digitally signed using signature schemes like DSA and RSA. This scheme consumes more computation due to finding new route and also applying signature schemes. The proposed scheme overcomes this limitations by applying the specification method to identify the intrusions at the earliest point.

B. Research Motivation

Table 1 classifies various attacks present in the wireless sensor networks. The intruders launch the routing attacks to degrade the network performance. The sinkhole attack is one of the major threat in the sensor network [6], since it can be made as a platform to launch further attacks like selective forwarding, wormhole and so on. The existing acknowledgement based schemes consumes more computation and energy, this motivates to develop a light-weight specification model. The proposed SEAACK applies specification detection model to identify the intruders in the network with minimum resource consumption.

IV. SYSTEM DESIGN

A. Problem Description

In Acknowledgement based schemes, there exists several problems like increased computation due to transmission of the acknowledgement packets, and there is a chance of fake misbehavior report generation. In the existing scheme EAACK, it adapts new route to verify the correctness of the misbehavior report. This increases the computation and make the method not suitable to WSN. The acknowledgment packets can also be forged. This problems exists in the literature and the proposed SEAACK scheme overcomes this problems by introducing the specification model to solve the problems in the existing acknowledgement based schemes.

B. System Architecture

The proposed specification model is explained in the following section. Fig.1 shows the IDS architecture. The source adapts the acknowledgement scheme for the transmission process. If the destination respond with the reply packet within the predefined time period, then the transmission is normal, otherwise it initiates specification process to confirm the presence of the malicious nodes. The following section explains the algorithms for this process.

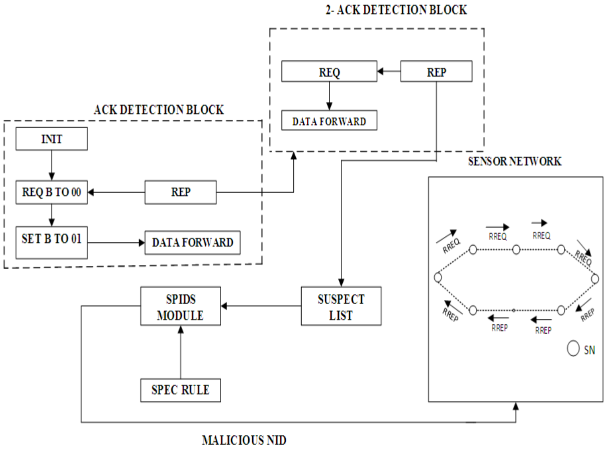

Fig. 1. IDS architecture.

ACKDET (T)

```
Initialize RT =0
    for i= 1 to n
        RT =RT+1
        BH = 00
    if RT>=T
        2-ACKDET ( )
    else
        return "Ack"
        BH = 01
```

Algorithm Description: Consider the sensor nodes SN1, SN2…..SN6 are the nodes in the network. SN1 is the source and intend to send data packet to the destination node SN6 through the intermediate nodes and transmit the packet with bit header set to 00. The reply timer is enabled and if, the transmission is normal, before the expiry of the timer the acknowledgement packet will reach the source from the destination with header 01. The intermediate nodes like SN2, SN3, SN4 and SN5 forward the packet to SN6. If, the intermediate node is malicious, then the acknowledgement packet doesn't reach the source within the timeout period and 2-ACKDET process is initiated to identify the malicious nodes.

2-ACKDET (REQ)

```
SN₁, SN₂ …. SNₙ are sensor nodes in the network
SN3 is the two – hop node
for i= 1 to n
specrule ( )
```

Algorithm Description: Consider the sensor nodes SN1, SN2, SN3, SN4, SN5 and SN6 in the network, in which SN1 is the source and transmit the data packet to the destination SN6. Source forwards the packet through the intermediate nodes. The node which is at two-hop away from the source should respond with the acknowledgement packet within the predefined time, if not then the source initiates the detection process to identify the malicious node.

Algorithm 3 Specrule ( )

Let node identifier (NID) be the specifier ID, Number of Message exchanged be the No. of connect, No. of dropped messages and No. of intermediate messages be the attribute_change, No. of forwarded requests be the System call, No. of generated requests be the Process, No. of data handling operation be the task executed, spec_max be the specification value and No. of data forwarding be the Pkt_operation.

Specrule (spec_max)

```
if attribute_change< System call && System call > Process
attr_max = minimum (System call, attribute_change)
attr_cal  = maximum (attr_max, Process)
attr_min = minimum (execute, Pkt_operation)
spec_max = maximum (attr_cal, attr_min)
if spec_max<= attribute_change
return NID "Sinkhole Node"
```

Algorithm Description: The algorithm Specrule ( ) follows the specification based methodology to detect the intrusions. The arguments used in the specification model are system call, process, task execute, packet operation, attribute change and so on. The node ID is equivalent to the specifier ID, system calls denotes the start and end of the events, process denotes the event in the queue for processing, attribute_change denotes the change in the behavior and in our case it is packet transmission, task denotes the process being executed, packet operation denotes the packets forwarded. The forwarder must be connected with the current transmitter. The specifications is generated as attribute_change must be less than system call and the system call must be greater than the number of process executed and the minimum value between the system call and attribute_change is selected as maximum attribute (attr_max), then the maximum value is compared with number of process executed as number of attr_cal. Now, the minimum value among execute and pkt_operation is compared with attr_cal and maximum value is selected to compare with the drop count as change of attributes. If, the change of attributes is greater or equal to the selected specification then the forwarder is identified as sinkhole node. The ID of the sinkhole node is broadcasted to the neighbor nodes and also reaches the BS (Base Station). The base station stores the malicious node ID in the BL (Black List) and broadcasts to the entire network. The sensor nodes receives the node ID of the malicious node and the node is removed from the routing table for further processing of the network.

V. SIMULATION ANALYSIS

The proposed model is simulated in NS-2. Table 2 shows the simulation setup.

To evaluate the performance of our proposed scheme with the existing EAACK the control overhead, delay, packet drop ratio, normalized overhead, packet delivery ratio, throughput and detection ratio is analyzed in the following scenario.

A. Scenario: Varying Node Density

Control overhead. The number of the control packets gives the control overhead. In Fig. 2, the proposed scheme has around 2% less overhead compared to the existing scheme EAACK scheme. Since, the number of control packets used by the proposed scheme is lesser, it achieves less overhead than the existing scheme.

Table 2: Simulation setup.

Sensor Nodes	100
Base Station	1
Transmission Range	100m
Initial Energy	100J
Probability	0.09
Slot_time	0.1
DROP_THR	10

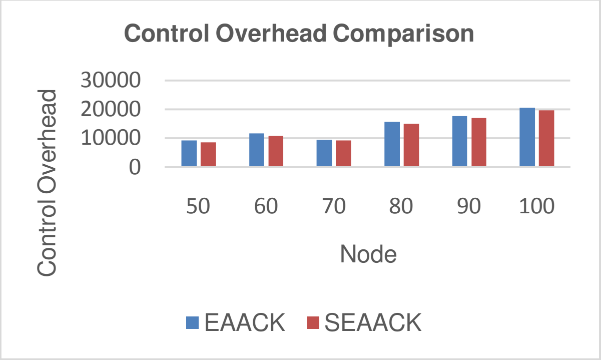

Fig. 2. Control Overhead comparison.

Delay. The ratio of difference between the finish time of the simulation and the start time of the simulation to the packets received gives the value delay parameter. In Fig.3, the proposed scheme SEAACK achieves around 12% lesser delay than the existing scheme EAACK. Since, the specification model doesn't take much time for threat analysis, the delay is lesser in proposed scheme compared to the existing scheme.

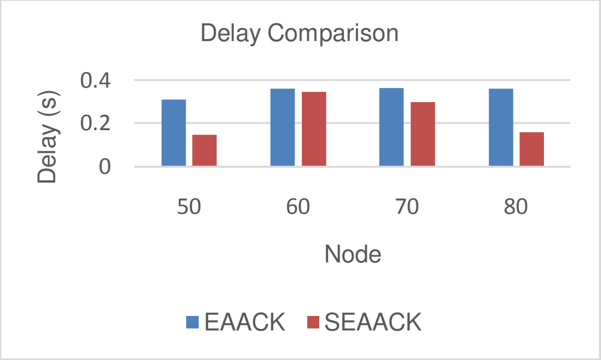

Fig. 3. Delay comparison.

Packet Drop Ratio. The ratio of the packets dropped to the packets send gives the packet drop ratio value. In Fig.4, the proposed scheme SEAACK achieves around 71% less dropping ratio compared to the existing scheme EAACK. This proves that the proposed scheme identify the malicious nodes and removes from the network which gradually reduces the packet drop ratio.

Normalized Overhead Comparison. The ratio of the control overhead to the packets received gives the normalized overhead. In Fig. 5, the proposed scheme SEAACK has around 16% less number of transmissions than the existing schemes like EAACK, so the normalized overhead is lesser in the proposed scheme.

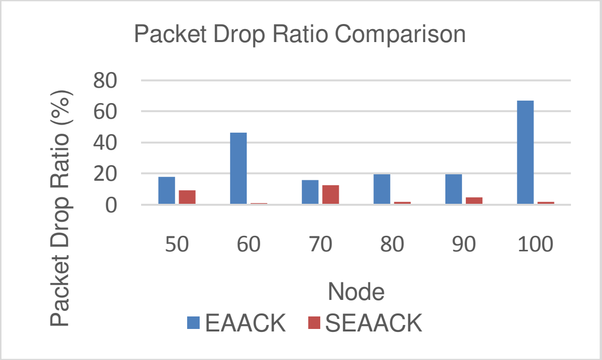

Fig. 4. Packet Drop Ratio comparison.

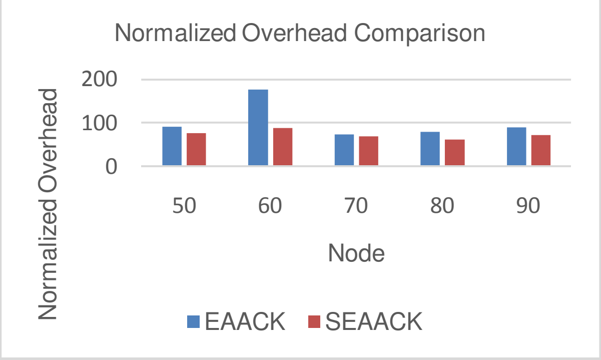

Fig. 5. Normalized Overhead comparison.

Packet Delivery Ratio. The ratio of the received packets to the packets sent gives the packet delivery ratio.

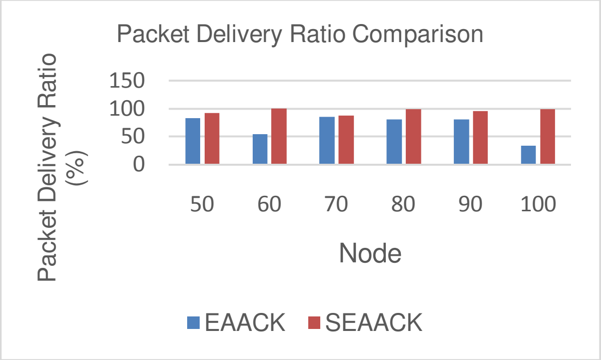

Fig. 6. Packet Delivery Ratio comparison.

In Fig.6, the proposed scheme namely SEAACK achieves 22% higher packet delivery ratio than the existing scheme EAACK. Since the malicious nodes are identified and removed, the packet dropping drops which increases the packet delivery ratio.

Throughput. The throughput is the ratio of the total packets received to the certain period of time. In Fig.7, the proposed scheme SEAACK has around 11% higher throughput compared to the existing scheme EAACK in terms of varying node density of the network. The identification of the malicious nodes is done quickly to avoid further damage to the network. Hence the malicious nodes are removed, the data transmission process is performed in a smooth manner and it increases the throughput of the network.

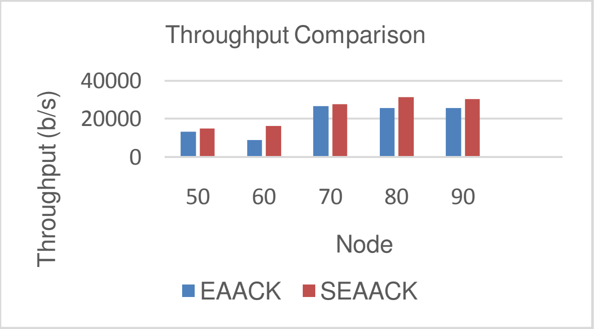

Fig. 7. Throughput comparison.

Detection Ratio. The ratio of detected attacks to the actual number of attacks gives the detection ratio. In Fig.8, the proposed scheme SEAACK scheme improves around 33% higher detection ratio than the existing scheme EAACK. Since, the proposed specification model has less number of operations, it identify the malicious nodes efficiently and it gives higher detection capability compared to the existing scheme.

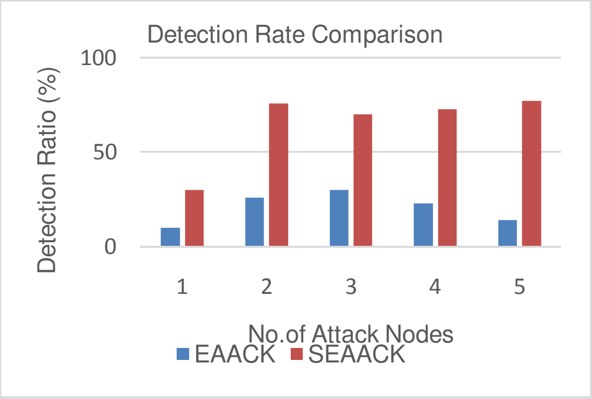

Fig. 8. Detection Ratio comparison.

VI. CONCLUSION AND FUTURE WORK

Wireless sensor networks is a resource constrained environment and security plays a major role in the performance of the network. Sinkhole attack degrades the network performance by dropping the packets and reduces the efficiency of network. The proposed SEAACK algorithm adapts Acknowledgement based specification intrusion detection mechanism and adds more security to the software safety of the sensor nodes in the sensor network by identifying the malicious nodes with minimum resource consumption, less packet drop ratio, higher packet delivery ratio and high throughput. This proposed scheme can be extended to protect Internet of Things environment. Further, the proposed specification model can be generically applied to other set of protocols in different environments.

ACKNOWLEDGEMENTS

The authors would like to acknowledge SASTRA University for the great support and assistance rendered to carry out this research work.

REFERENCES

[1]. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. In *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003.* (pp. 113-127). IEEE.

[2]. Liu, K., Deng, J., Varshney, P.K., &Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. *IEEE transactions on mobile computing*, (5), 536-550.

[3]. Uppuluri, P., &Sekar, R. (2001). Experiences with specification-based intrusion detection. In *International Workshop on Recent Advances in Intrusion Detection* (pp. 172-189). Springer, Berlin, Heidelberg.

[4]. Sheltami, T., Al-Roubaiey, A., Shakshuki, E., & Mahmoud, A. (2009). Video transmission enhancement in presence of misbehaving nodes in MANETs. *Multimedia systems*, **15**(5), 273-282.

[5]. Shakshuki, E. M., Kang, N., &Sheltami, T. R. (2012). EAACK—a secure intrusion-detection system for MANETs. *IEEE transactions on industrial electronics*, **60**(3), 1089-1098.

[6].Krontiris, I., Dimitriou, T., Giannetsos, T., &Mpasoukos, M. (2007). Intrusion detection of sinkhole attacks in wireless sensor networks. In *International symposium on algorithms and experiments for sensor systems, wireless networks and distributed robotics* (pp. 150-161). Springer, Berlin, Heidelberg.

[7]. Marti, S., Giuli, T.J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 255-265). ACM.

[8]. Hai, T.H., Huh, E.N., & Jo, M. (2010). A lightweight intrusion detection framework for wireless sensor networks. *Wireless Communications and mobile computing*, **10**(4), 559-572.

[9]. Ishmanov, F., Kim, S., & Nam, S. (2014). A secure trust establishment scheme for wireless sensor networks. *Sensors*, **14**(1), 1877-1897.

[10]. Liao, H.J., Lin, C.H.R., Lin, Y.C., & Tung, K.Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, **36**(1), 16-24.

[11]. Djenouri, D., &Badache, N. (2009). On eliminating packet droppers in MANET: A modular solution. *Ad Hoc Networks*, **7**(6), 1243-1258.

[12]. Chae, Y., DiPippo, L.C., & Sun, Y.L. (2012, October). Predictability trust for Wireless Sensor Networks to provide a defense against On/off attack. In *8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)* (pp. 406-415). IEEE.

[13]. Govindan, K., &Mohapatra, P. (2011). Trust computations and trust dynamics in mobile adhoc networks: A survey. *IEEE Communications Surveys & Tutorials*, **14**(2), 279-298.

[14]. Yu, H., Shen, Z., Miao, C., Leung, C., &Niyato, D. (2010). A survey of trust and reputation management systems in wireless communications. *Proceedings of the IEEE*, **98**(10), 1755-1772.

How to cite this article: Sundararajan, R.K., Narendran, S.M. and Umamakeswari, A. (2019). Specification Based Intrusion Detection Mechanism for Mitigating Sinkhole Attack in Wireless Sensor Networks. *International Journal on Emerging Technologies*, **10**(2): 462–466.