A Cluster-Based Mitigation Strategy Against Security Attacks in Wireless Sensor Networks

Jahangir Khan[1]
Community College
Department of Information Systems
King Khalid University, Tehama Branch
Kingdom of Saudi Arabia

Ansar Munir Shah[2]
Department of Computer Science and IT
Institute of Southern Punjab (ISP)
Multan, Pakistan

Babar Nawaz[3]
Department of Computer Science
IIC University of Technology
Phnom Penh
Cambodia

Khalid Mahmood[4]
College of Science and Arts
Department of Information Systems
King Khalid University Tehama Branch
Kingdom of Saudi Arabia

Muhammad Kashif Saeed[5]
Community College
Department of Information Systems
King Khalid University, Tehama Branch
Kingdom of Saudi Arabia

Mehmood ul Hassan[6]
Department of Computer Skills
Najran University
Kingdom of Saudi Arabia

***Abstract*—Wireless Sensor Networks (WSNs) applications range across distinct application comprising of event detection at real-time. WSNs can be deployed for not only mobile nodes but also for static sensor nodes (SNs) for various applications which may include health care system, smart parking, environmental monitoring etc. Sensor nodes in WSN are constrained in terms of energy contents of each node and can be accessible by other nodes in a wireless medium are more likely to be susceptible to various categories of attacks. Wireless Network are more likely prone to various kinds of security attacks, one such type of attack caused by a malicious attacker, which can result to decay in the lifetime of the network and an adverse scenario can even lead to congestion in the entire network. This paper presents the overview of various attacks and their consequences on different layers and evaluates defense strategy used to mitigate the various categories of attacks on Wireless Sensor Networks. This study proposes a cluster-based approach for each node of a WSN where the nodes of network constrained by energy can organize and perform network duties as per the network performance for this one node performs the role of cluster head (CH) which is elected on the basis of the "Reputation" of a node which is an indicator of nodes individual behavior in the network and "Net_Credit_Score" which determines the cooperating behavior of sensor node in the cluster. Further, this study highlights few parameters which can be implemented to further enhance the defense strategy by taking into account the factors such as Cluster count, Stability factor of both the Cluster and Cluster Head and Intra-Cluster topology which can be crucial. This will result in formulating a road map for designing a secure and resistant reputation-based system for WSN to overcome the various security related attacks.**

***Keywords*—Wireless sensor network; security attacks; security issues; clusters**

I. Introduction

Wireless Sensor Networks (WSN) can be defined as a versatile communications system that makes use of the wireless medium (radio frequency) in order to transmit and receive data, therefore reducing their dependency on wired connections. It can be termed as a group of spatially dispersed and dedicated sensors deployed to monitor and collect the details such as the physical conditions existing in a region such as the collection of data, scientific examination, military applications etc. But the sensor nodes are constrained due to various factors such as security issues and limited resource energy; they are more likely to be vulnerable to security attack.Security threats can easily affect the WSNs. Sensor network attackers donot need to constrained by the characteristic of sensor nodes since they are able to use costly transceivers and power supply nodes, making it possible for this type of network to be affected. The local storage ability of sensor network is very minmal [1], so in order to run very complex cryptology protocols, security mechanisms for sensor networks can not enable each sensor node to store long-sized keys. Sensor nodes have low power consumption, so power preservation must be the priority of sensor network protocols. Usually, sensor networks comprise of a huge number of communication nodes, do not have a global identification number and might face simple node failure.

The purpose of the attacker is to render target domains inaccessible to legitimate users. In several areas a sensor network without adequate security against attacks will not be deployable. Wireless networks are more vulnerable to security attacks due to the transmission medium being broadcasting in nature. The security attacks [2] are the situation of violation of

system security, carried out by an intelligent entity and is a deliberate act of threat on an organization(system) resource or service. We need to design a security algrorithm for secure working condion.

This paper considers cluster-based strategy for mitigation against security attacks carried out on WSNs and proposes a cluster-based approach which is Fault-tolerant and by categorizing the sensor nodes into cluster also considers the balancing of network load.

The paper is organized as follows. In Section II we present related work to various security attacks in detail. The Security requirements of WSNs is explained in Section III. Section IV gives a review of attacks on WSN. A proposed cluster-based mitigation strategy is described in Section V. Section VI presents conclusions and future enhancements related to security attacks on WSN have been considered.

II. Related Work

The paper [3] examines and evaluate the various kinds of attacks carried out on WSN. The main focus of this study is to examine how such attacks can be prevented for WSNs by creating a sound understanding of various kinds of attacks in WSNs. In [4] the authors have conducted a review on DDoS attack to present its impact on networks and to present various defensive, detection and preventive measures which can be adopted in order to mitigate attacks on WSNs. Various parameters related to methods used for selection of clusters [5] need of re-clustering [6] and study of the QoS parameters such as performance [7] of nodes in WSN. The approach used in [8] determines that the cluster head is selected on the basis of a threshold value "T" which can be calculated using the remaining energy and relative position of the node in the network. In the study [9] CH is elected based on assigning weight factor to the nodes such as Reputation-based system such as RFSN [10] and DRBTS [11], energy, mobility and distance between the nodes and based on the weighted value of these three parameters Cluster head can determine.

1) Physical layer: The attack primarily focused on this layer that may affect (leading to starvation) or may not affect (resulting in sniffing) the physical environment needed to send the data.

2) Data link layer: DDoS attacks (active as well as passive) can be carried out resulting in increase in the packet drop or in adverse situation may even lead to decrease in the lifetime of the network.

3) Network layer: Sniffing attack and intelligently carried out DoS attacks (that allow the traffic to pass through it) and then ultimately slowly increasing the magnitude to block the route(congestion)on increase the magnitude of the attack.

4) Transport layer: Denial of service attack at this layer is aimed to make use of the information of the network resources(machines) working, the main aim of the attack is to cause adverse impact leading to halt in the working(congestion) of the entire network. Both online, as well as offline services, are likely to be affected through this attack.

5) Session and presentation layers: Till date, any attack mainly targeting these layers have not been discovered.

6) Application layer–This layer disclosed to both active as well as passive attacks. Distributed denial of service is common at this layer.

Table I presents various types of attacks at the multiple layers. The consequences of these attacks depend on the impact caused by the outcomes of the resources affected by these attacks.

Table II presents various protocols, one of the strategy is to monitor the malicious characteristic of nodes on the basis of Non-Cooperative nodes. So in order to mitigate the attacks on the wireless network, we have taken into account the malicious activity shown in terms of the non Cooperating behavior characteristics exhibited by the nodes of the network. Algorithm 2 describes assigning of Reputation value to each sensor node of the network. One method to identify non-cooperative nodes is to assign a "Node_Reputation ( )" value to each of the node cooperating in the transmission process. Since each node in Mobile Adhoc networks and WSNs have no other way of collecting the information about the nodes located outside their range, and therefore there is a greater chance of uncertainty in the communication information related to them. So in order to enhance trust and reputation - based system for MANETs and WSNs in particular is a challenging issue. MANETs are assumed to be self-configuring collection of nodes mobile in nature connected by wireless links. These nodes are exhibit random movement and is the primarily the reason for rapidly changing topology of the network.

Load balancing [12] in WSN is critical to classify the sensor node into equal size groups so as to ensure that expected network performance is achieved for each node, Fault tolerance [13] is the feature of a network which ensures reliability and trust aspect of dependency of each sensor node on other nodes of the network.

TABLE I. DDoS Attacks at Various Layers in Wireless Sensor Network

Layers	Types of Attacks	Consequences of Attacks	Impact of Attack
Physical	Sniffing	Nodes exhibiting malicious pattern	Mild
	DDoS	Starvation, Depletion of Resources	Severe
	Tampering (node capturing)		
Data Link	Active DDos Attacks	Increase in packet Drop Ratio	Mild
	Passive DDoS Attacks	Decrease in lifetime of network	Severe
Network	Sniffing	Nodes exhibiting malicious pattern	Mild
	DOS	Congestion	Severe
Transport	DoS	Congestion	Severe
Session and Presentation	No attack noticed yet	---------	---------
Application	Sniffing	Loss of Packests	Mild
	Spoofing (IP, ARP, DNS	Delay in the packets transmitted	Severe
	DDoS	Lifetime Decay	Severe

TABLE II. DEFENSE SCHEME USED AT THE VARIOUS PROTOCOL LAYERS

Protocols Layers	Types of Attacks	Defense Used
Physical	Node Destruction	Hide Nodes
MAC (Medium Access Control)	Denial of sleep	Sleep
Network	Spoofing	Authentication
	Hello Foods	Geographic Routing
	Homing	Header Encryption
Transport	SYN flood	SYN Cookies
	Desynchronization	Path Authentication
Application	Path Based DoS	Anti-replay protection
	Reprogramming Attacks	

In these networks, each node plays the dual role of being the end-system as well as the task of relaying the packets to the other nodes. Since the nodes in MANET are autonomous without any common interest, so there is a greater tendency for a node to not participate in a cooperative manner with other nodes of the network. This Non-cooperative behavior exhibited by the node explained in Fig. 1 may lead to malicious activities such as leading to DoS (Denial of service) attacks and various other deviation from ideal expected behavior by the sensor node.

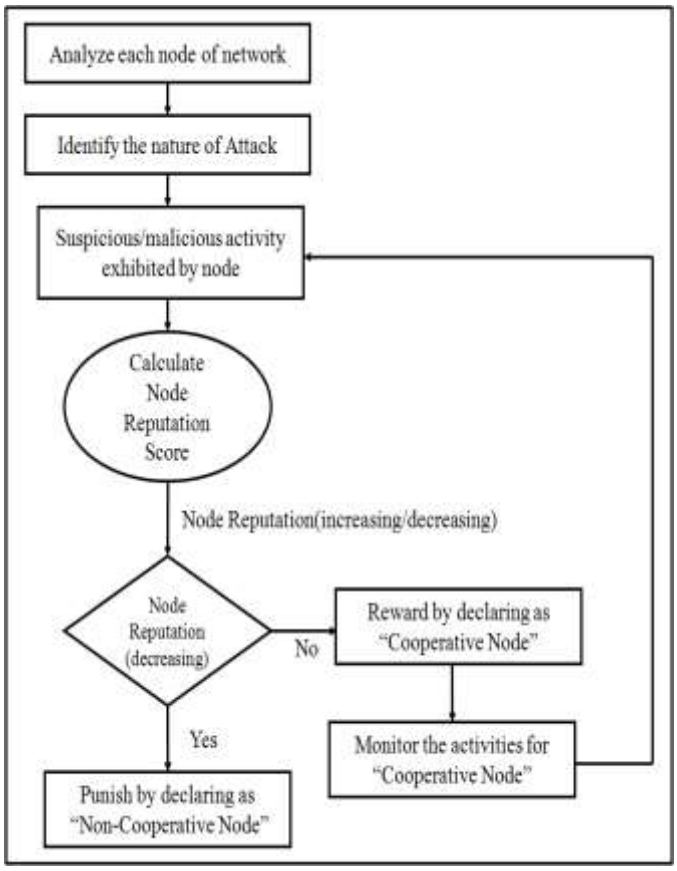

Fig. 1. Identification of Node Behavior in Wireless Sensor Network.

Unlike MANET, in case of WSNs all the sensors nodes are confined to be the part of a single group and they operate to attain same goal. So there arise a need to classify the nodes of WSNs into groups called "Clusters".

III. SECURITY CONCERNS IN WSNS

WSNs have been emerging as the most widely deployed networks in various application areas. The Security concern for WSNs are as follows [14][15]:

A. Confidentiality

It is the measure which assures that sensor nodes control or influence what information related to them may be collected and stored and by whom (sensor nodes) and to whom that piece of data or information may be disclosed.

B. Integrity

It is the measure which ensures that the data or information received by a sensor node must not be altered maliciously by the member nodes of WSNs.

C. Authentication

It is the measure which ensures that the entity (sensor node) being a genuine member of the network which can be trusted and verified against the data sent and received being the legitimate sender and receiver of the data or information.

D. Authorization

The authorization is used to ensure and assure that only the authorized (legitimate) sensor nodes are allowed to perform the required operations in WSNs.

E. Availability

It is the measure which ensures that information access is on a timely basis and reliably that is WSN services must be available whenever the WSN users need them.

F. Secrecy (Forward and Backward)

Forward secrecy is deployed in WSN in order to disallow a sensor node that has left a Wireless Sensor Network from accessing (read) any future data,whereas Backward secrecy means preventing a new incoming sensor node to a Sensor Network from reading any previous data.

IV. ATTACK ON WIRELESS SENSOR NETWORKS

There are wide ranges of attacks. Fig. 2 presents security attacks that are classified as passive attacks and active attacks.

A. Passive Attacks

In Passive attacks, the main goal of the intruder (opponent) is to monitor (examine) and obtain the information that is being transmitted between the sender and the receiver. These are the attacks against the privacy of wireless sensor network. Some of the passive attacks are the release of message contents, eavesdropping and traffic analysis, etc. In addition to these various attacks aimed to obtain various critical information such as decoding the poorly enciphered traffic, and observing the important information such as secret message and identification. The consequence of these attacks is the exposure of information or any feasible source of data to an attacker.

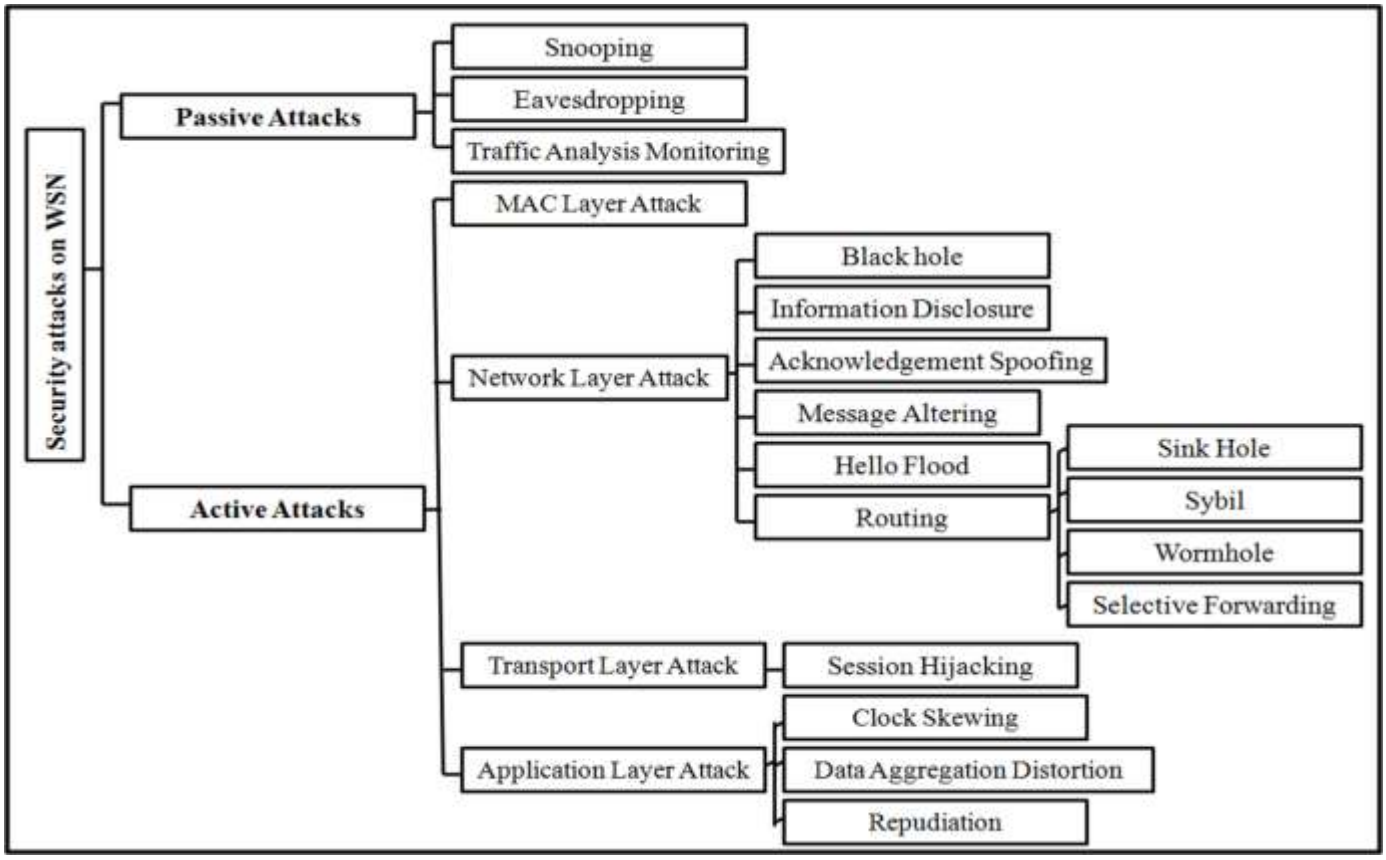

Fig. 2. Classification of Security Attacks for Wireless Sensor Networks.

B. Active Attacks

Active attacks are mainly targeted with primary aim leading to the modification of the data stream or the creation of a false stream in order to disturb their operations. The attacker alters the data stream to masquerade one entity as some other. As a result of Active attack may be the exposure of data files and their amendment or in worst scenarios may even lead to denial of service (DoS). Various detection and prevention methods can be used to avoid multiple DoS attacks. A DDoS attack is initiated by flooding a massive number of data packets or bogus requests to a victim's network that leads to increase the bandwidth requirements. Therefore, exceeding beyond the capacity of handling the application by the victim(server), so that the processing node is flooded with undue requests that prevent legitimate users from receiving the service and hence leads to congestion or starvation [16], [17].

Such types of attacks target both the service provider and user in addition the main resources for attack can be aimed to disrupt the processing unit or the memory, to drain the energy of the sensor node(battery power), and the bandwidth of the wireless network. These attacks also affect connectivity and reduce the throughput and quality of service (QoS). As the sensor nodes of WSNs continuously monitor the dynamically changing parameters in the network. Therefore any issue such as packet drop etc. is shared with the neighbouring nodes, based on such information possibility of a kind of denial of service attack can be identified and due to preventive measures can be adopted by the nodes of WSNs.

V. PROPOSED WORK

Many studies over recent years have summarized the role of various parameters related to methods used for selection of clusters need of re-clustering and study of the QoS parameters such as performance of nodes in WSN. Some approaches uses the concept that the cluster head is selected on the basis of defining a threshold value which can be calculated based on critical parameters such as residual energy and relative position of the node in the network. In this study CH is elected (given in Algorithm 1) on the basis of selecting the maximum value of Reputation and Score of an individual node and Cluster head, respectively.

Algorithm 1: SELECTION OF CLUSTER HEAD IN WIRELESS SENSOR NETWORK

Score-Scr
Reputation-Rep
Node-Nod
$\mathbf{S_m}$- varaiable assigning maximum value of scr
$\mathbf{R_m}$ – variable assigning maximum value of rep
Value-Val
ClusterHeadSelection ( )
{
Scr = NodScrVal ( )
Rep=NodRep ( )
S_m=Max(Scr( ))
R_m=Max(Rep( ))
For each cluster $C_j \epsilon$ WSN
{
For (each node N_i && N_i = 1 to N_i = n)
{
If (S_m || R_m)
{
Set Nod N_i as $(CH)_j$
// i^{th} nod is assigned to the j^{th} cluster as CH
}
else
{
Add node j^{th} Cluster i.e. C_j
}
}
}
}

Identifying the nodes of WSN into clusters can lead to attain the objectives, namely, as:

A. Load Balancing

Load balancing of nodes in a WSN is a measure of the distribution of the various overheads related to data processing or various other intra-cluster management task confined to the cluster head (CH) node within the network. So there arise a need to maintain a balance of the load among the nodes of a WSN, so that every node can meet its expected performance goals. Specifically for WSN where the CH are to be selected among the sensor nodes of the network. Therefore formulation of "Cluster" is crucial in order to extend the lifetime of the network and meet the expected performance criteria.

B. Fault-Tolerane

As WSNs are expected to operational in extreme and adverse working situations such as military applications such as battlefield surveillance, border surveillance, Disaster management, security surveillance etc. therefore these networks are likely to suffer from physical damage and malfunction etc. Failure of a node of WSN can have a significant impact on the network and this situation can worsen if the affected node is a cluster head, as the loss or failure of a CH means loss of certain critical sensor data. So we need an intuitive way to overcome the overcome the failure of a Cluster Head.

Algorithm 2. REPUTATION-BASED CREDIT SCORE OF A NODE OF A CLUSTER IN A WIRELESS SENSOR NETWORK

Nod_Rep ( )
{
For each nod $N_i \epsilon$ WSN
Each node maintains **(Nod_id, Net Rep_Scr)**
//Where **Net_Rep_Scr = S_credit-U_credit**
If (S_Credit >= U_Credit)
{
Net_Rep_Scr val Increases
}
Else
Net_Rep_Scr val Decreases
}
where
Nod_id – Nod id in the cluster
S_credit – score corresponding to correctly Packet forwarding capability of a node
U_credit – is score corresponding to Un- correct forwarding capability of a node

S_credit(A,B) = +ive value // Successful _Credit_Score

U_credit(A,B) = -ive value // Unsuccessful _Credit_Score

//**Net_Credit_Scr** which represents its reputation and is calculate as

Net_Credit_Scr = $\sum$**S_Credit(i , j)** + $\sum$**U_Credit(i , j)**
// where nod "i" is request for service from "j"

If (Net_Credit_Scr >= 0)
{
Nod has + rep.
}
else
{
Nod is consider malicious nod
}
rtn(Net_Credit_Scr);

In this study, we have considered incentive (based on *Reputation_Score()* of a node of the network) based approach can be used to enhance trust for nodes in WSNs to behave in a cooperative manner. Many Reputation and trust-based systems based system has been successfully modelled for WSNs. WSN is an autonomous collection of mobile nodes driven by constrained resources such as energy content of node so in order to enhance the network lifetime is a major concern. In order to address issues such as scalability, energy of a node, the nodes are often grouped into disjoint clusters. Each cluster is monitored by a node referred as cluster head (CH).The selection of Cluster Head is based on calculation

"Node_*Reputation( )"* which is the characteristics of individual sensor node of WSN where as *NodeScoreValue( )* which is the characteristic of node behavior in the cluster.

VI. Conclusion

In this work, we have proposed cluster-based mitigation technique basis of *Net_Credit_Score* assigned to the nodes of a wireless sensor network. A positive "*Net_Credit_Score"* increases the trust & Reputation of a sensor node among the nodes of a WSN, whereas a negative value is an indicator of nodes exhibiting malicious or suspicious behavior. Some of the critical factors which can be considered for future work can be the constrained energy of sensor node of WSN, as the power of each sensor node is limited the network lifespan of WSN is critical issue to consider. Similarly, Cluster count (i.e. size of cluster), Stability of Cluster and Cluster Head and Intra-Cluster topology can also be some critical parameters to consider in devising strategies for mitigating against the security attacks carried out on WSNs.

Acknowledgment

The authors would like to express their gratitude to King Khalid University, Saudi Arabia for providing administrative support.

References

[1] I. F. Akyldiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, “Wireless sensor networks: a survey,” Computer Networks, vol. 38, 2002, pp:393-422.

[2] Khan, Rizwan, and A. K. Vatsa. "Detection and control of DDOS attacks over reputation and score based MANET." Journal of Emerging Trends in Computing and Information Sciences 2.11 (2011): 646-655.

[3] Upavi .E.Vijay1, Nikhil Sameul2, "Study of Various Kinds of Attacks and Prevention Measures in WSN", International Journal of Advanced Research Trends in Engineering and Technology (IJARTET),Vol. II, Special Issue X, March 2015.

[4] Sonali Swetapadma Sahu et.a. "Distributed Denial of Service Attacks: A Review", IJ Modern Education and Computer Science, 2014, 1, 65-71 Published Online January 2014 in MECS.

[5] Bhaskar P. Deosarkarl, Narendra Singh Yada and R.P. Yadav, 2008. Clusterhead Selection in Clustering Algorithms for Wireless Sensor Networks: A Survey, Proceedings of the 2008 International Conference on Computing, Communication and Networking (ICCCN 2008), 2008 IEEE.

[6] Ramesh, K. and Dr. K. Somasundaram, 2011. A Comparative Study of Clusterhead Selection Algorithms in Wireless Sensor Networks, International Journal of Computer Science & Engineering Survey (IJCSES) 2(4).

[7] Dechene, D.J., A. El Jardali, M. Luccini and A. Sauer 2010. A Survey of Clustering Algorithms for Wireless Sensor Networks, Network-Based Information Systems (NBiS), 2010 13th International Conference on Networking & Broadcasting, pp: 14-16.

[8] Hyung Su Lee, Kyung Tae Kim and Hee Yong Youn, XXXX. A New Cluster Head Selection Scheme for Long Lifetime of Wireless Sensor Networks, School of Information and Communications Engineering, Sungkyunkwan University, Korea.

[9] Saaty, T.L., 2000. Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process, RWS Publications, USA.

[10] A. Srinivasan, J. Teitelbaum, and J.Wu, DRBTS: Distributed reputation-based Beacon trust system, in Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing

[11] (DASC'06), Indianapolis, USA, pp. 277–283, 2006.

[12] S. Ganeriwal and M. Srivastava, Reputation-based framework for high integrity sensor networks, in Proceedings of the 2nd ACMWorkshop on Security of Ad Hoc and Sensor Networks (SASN '04), NewYork, USA, October 2004, pp. 66–77.

[13] Alam, M., & Varshney, A. K. (2016). A new approach of dynamic load balancing scheduling algorithm for homogeneous multiprocessor system. International Journal of Applied Evolutionary Computation (IJAEC), 7(2), 61-75.

[14] Gholamreza Kakamanshadi, Savita Gupta, and Sukhwinder Singh. 2015. A survey on fault tolerance techniques in Wireless Sensor Networks. In Proceedings of the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (ICGCIOT '15). IEEE Computer Society,USA,168–173.

[15] Reddy Y.B. A game theory approach to detect malicious nodes in wireless sensor networks; Proceedings of the Third International Conference on Sensor Technologies and Applications (SENSORCOMM); Athens, Greece. 18–23 June 2009; pp. 462–468.

[16] Agah A., Asadi M., Das S.K. Prevention of DoS Attack in Sensor Networks using Repeated Game Theory; Proceedings of the ICWN; Las Vegas, NV, USA. 26–29 June 2006; pp. 29–36.

[17] K. Giotis, M. Apostolaki, and V. Maglaris, "A reputation-based collaborative schema for the mitigation of distributed attacks in SDN domains," Proc. NOMS 2016 - 2016 IEEE/IFIP Netw. Oper. Manag. Symp., no. Noms, pp. 495–501, 2016.

[18] R. Wang, Z. Jia, and L. Ju, "An entropy-based distributed DDoS detection mechanism in software-defined networking," Proc. - 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2015, vol. 1, pp. 310–317, 2015.