# Detect and Prevent the Selective Drop Attacks in WANET's Using Resistive To Selective Drop Attack (RSDA) Scheme

**[1]KUMANA NARAYANA RAO , [2] M.SAMPATH KUMAR**

[1]M.Tech Student, Department of Computer Science and Systems Engineering, Andhra University, Visakhapatnam, AP, India

[2]Proffessor, Department of Computer Science and Systems Engineering, Andhra University, Visakhapatnam, AP, India.

## ABSTRACT:

The process of sending dedicated packets from one location to another location under a valid path is known as routing. As we all know that there are different types of routing techniques available in the real time network, where every technique depends on shortest path as the main factor. In a wireless sensor networks, the data will be transferred under a dedicated path which is given by the router and this path will be dynamically changes due to the mobility. During the data transfer they may occur some attacks by the intruders who try to stop the packets not to reach the destination or sometimes they want to delay the packets transfer. These type of attacks are not identified dynamically in the current wireless sensor networks or MANET's.Hence in this current thesis we try to investigate the problem of localizing node failures in communication networks with the help of binary states (normal/ failed) and try to find out the end to end delay and performance during data transfer. In this proposed paper, we present a Resistive to Selective Drop Attack (RSDA) scheme which can protect the sensitive data not to be dropped or revealed by the intruders who try to hack the data during data transfer; this will be act as a protective layer which provides security against selective drop attack. This RSDA protocol will try to protect the data from the intruders who try to create any type of attacks in the network, by providing an alternate path from the Point of Attack (POA) and can able to send the data packets in alternate best path. By conducting various experiments on our proposed method, our simulation results clearly state that our proposed approach will try to provide positive data transfer and try to find out the end to end measurements like delay, throughput, overhead and energy loss.

***KEYWORDS:***

Resistive, Selective Drop Attacks, MANET's, Wireless Sensor Networks, Node Failure, Delay Performance.

## I. INTRODUCTION

Wireless Sensor Networks is a collection of several nodes ranges from a few to several hundreds and even thousands of nodes, where each and every group of nodes is connected either to

Single sensor or group of sensors. A wireless sensor network is mainly formed by integrating several number of components like which is shown in figure 1.

1. A radio transceiver device with an inbuilt internal antenna or device connected to an external antenna.
2. A microcontroller
3. An electronic circuit board for interfacing mainly with the sensors and an energy source, usually a battery or an embedded form of energy harvesting.

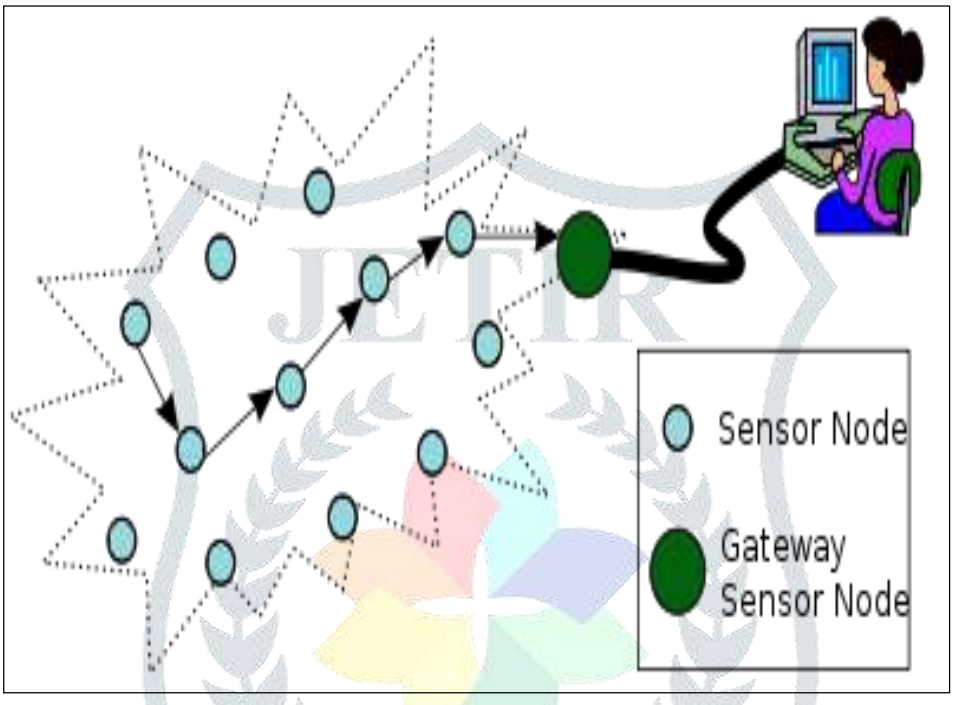



**Figure .1. Represents the Typical Multi-Hop Wireless Sensor Network Architecture**

These sensors will be gradually varied from one with other in its appearance, structure, size and its other parameters. Some of the sensors are shoebox down to the size of a grain of dust. In order to construct a WSN, we need to purchase at least single sensor nodes which has variable in its price, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. During the process of sensor deployment we need to use some resources like energy, memory, speed and bandwidth mainly depends on size and cost of the sensor what we use [1], [2].In current days there was a lot of research efforts made to develop a sensor network which contains a hardware and network architecture in order to deploy the WSNs.

In the field of information technology and data communication, WSN are an active research area with numerous workshops and conferences arranged each year for the improvement of its performance **[**3] – [6]. For the general purpose network deployment, normal WSN cannot able to fulfil the needs like sensing range, transmission**.** Mobile Adhoc Network is becoming more and more widely implemented in the industry.

In general the open nature and remote distribution of MANET networks will leave the attacks vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious [5], attackers can easily compromise MANETs by inserting malicious or non-cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs. Many research efforts have been devoted to such research topic [6].

## II. LITRATURE SURVEY

Literature survey is that the most vital step in software development process. Before developing the tool, it's necessary to work out the time factor, economy and company strength. Once this stuff is satisfied, ten next steps are to work out which OS and language used for developing the tool. This literature survey is mainly used for identifying the list of resources to construct this proposed application.

**MOTIVATION**

Two well-known authors Jiawei Li, and Athanasios [5], have written a paper on "Preventing Distributed Denial-of-Service Flooding Attacks with Dynamic Path Identifiers". In recent days almost all the network administrators try to find out the importance of path identifiers (*PIDs*) as inter- domain routing objects. These PIDs are almost static in nature and where the attacker try to create some sort of attacks within the network and they want to stop the packets not to be enter under the dedicated path,so this motived the authors to proposed dynamic PIDs in which the data can be send from valid source to destination under dynamic path and the data which is send from source to destination node are dynamic in nature and hence there will be an alternate path immediately if there is any attack found within the network.

Two well-known authors Issam Aib and Raouf Boutaba [6], have written a paper on "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks".In this paper the authors mainly discussed about the DDoS attacks which are exist in the distributed networks and how hard to find out those attacks in the network. In general these attacks are sometimes detected early and sometimes they become challenge to identify those attacks and take necessary step to protect the end users. The core nature of the proposed FireCol is composed of Intrusion Prevention Systems (IPSs) which is located in the ISP level. The evaluation of FireCol using extensive simulations and a real dataset is presented, showing FireCol effectiveness and low overhead, as well as its support for incremental deployment in real networks.

An Intrusion detection system (IDS) is internet software which is mainly deployed on the hardware designed to detect any unwanted attempts to access, manipulating, and/or disabling of computer mainly through a network [14],[15]. An intrusion detection system is mainly used to identify several types of malicious behaviors that can easily compromise the security and trust of a computer system. Some of the attacks include network attacks against vulnerable services, host based attacks such as privilege escalation attack, unauthorized logins attack and attempting to access some invalid files like viruses and worms[13].

An IDS is mainly composed of several components:

1. **SENSORS**: This is used for generating security events.

2. **CONSOLE**: Which is used to monitor events and alerts, while controlling the sers?

**3. CENTRAL ENGINE**: Which is mainly used for recording the events logged by the sensors in a database and use a system of rules to generate alerts from security events received.

## III. PROPOSED NOVEL RSDA SCHEME FOR ATTACK DETECTION

In this section we will mainly discuss about proposed Novel RSDA (Resistive to Selective Drop Attack) approach for identifying the selective drop attacks which is created by the intruder within the network during data communication in a wireless sensor networks. Now let us discuss about this proposed model in detail as follows:

### MOTIVATION

The main motivation behind this detection of selective packet dropping attacks is to find out the packet drop attacks that were created by a malicious node inside the network. Initially we assume that links on the current path of our network exhibit the natural packet loss and there may be several adversary nodes that may present in the network during data transmission [8]. In general during the data transfer some nodes may become failed due to its internal functionality and some nodes may become attacked due to the external attacker who try to create attacks inside the network. For simplicity, we try to assume only linear data flow paths (i.e., as shown and described in Fig. 2a). Also, in this section we don't address the issue related to recovery of node once a malicious node is detected. All the Existing techniques that are available in the literature are almost orthogonal to our detection scheme and they may initiate multipath routing [9] when any compromised nodes occur within the network during the data transfer in one best path.

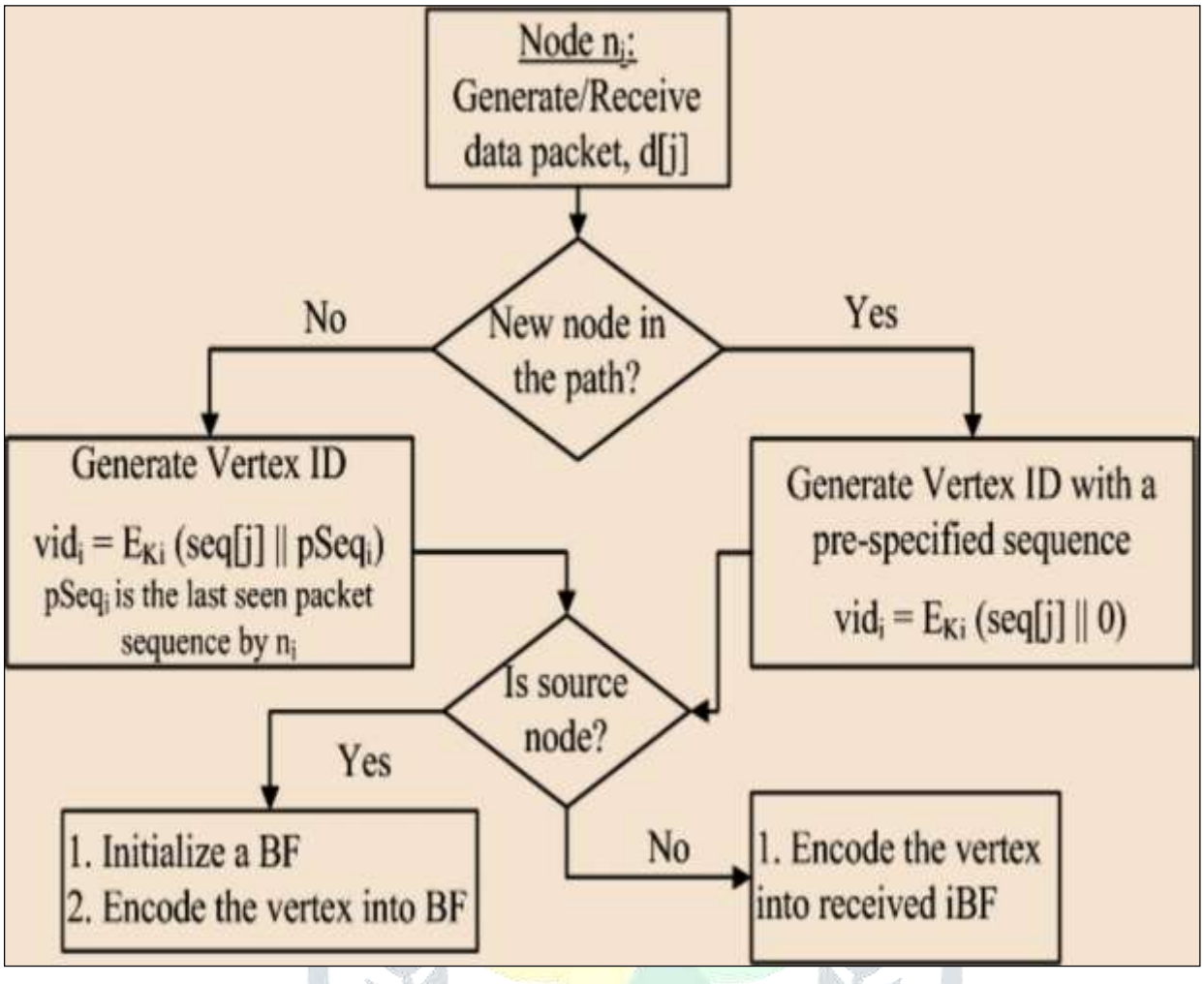



**Figure 2 .Represents the proposed approach to Detect Packet Drop Attacks And Identify Malicious Nodes inside a WSN**

Initially we try to prove the method of data provenance encoding for the packet acknowledgement that requires the sensors to transmit more meta-data. For each and every data packet ,a provenance record will be generated by a node and it will contains mainly of node ID and an ack for the node in the form of a unique sequence number of the last seen delivered or forward packet[10]. During the process of data transfer from one node to other node if there was any packets dropped due to intermediate nodes failure then we can identify some nodes only can participate in sending the packets from valid source to destination and some are in active state of not carrying any data packets[11]. For this we consider a flow of data oath with term like “P” and n1 is nothing but the data source and we denote the link between the nodes n1 to ni as the li.

From the above figure, we can clearly find out the process of extended provenance encoding process. If we look at the figure in detail, each and every provenance record for a certain node includes the following fields like

1) The node ID,
2) An Acknowledgement of the last seen packet flow.

The Ack for the packets can be generated in several ways to serve this purpose. In our solution, a node ni creates a vertex vi for every jth packet it generates/forwards. The vertex $ID_{vidi}$ is generated as follows:

$$vid_i = generateVID(n_i, seq[j], pSeq_i) = E_{K_i}(seq[j] \,||\, pSeq_i),$$

Where the fields like **pSeqi** is the knowledge of ni(i.e. Data provenance Update) about the sequence number of the previous packet in the flow.

**ni** is defined as the updates of the data provenance for the packet by inserting vidi into the iBF.

## IV. IMPLEMENTATION STAGE

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. The front end of the application takes Awt, Swings, Socket programming and as a Back-End Data base we took My SQL data base. The application is divided mainly into following 5 modules. They are as follows:

### 1. SENDER MODULE

In this module, the sender node will try to browse the file, select the destination and sends to the router. In this sender window the sender has the option to upload the file and encrypt the file and then try to upload the file in a secure manner. The sender need to choose the valid destination node and then try to choose valid ip address for sending the data to the destination nodes.

### 2. ROUTER MODULE

In this module, router will try to contain a set of intermediate nodes which is mainly divided into four clusters, where each and every cluster will contains a set of intermediate nodes. Initially the source node will try to choose a valid text file as input and then same file will be divided in the form of packets and these packets will be received by the router and now the router will generate a best path and send the data packets to the valid destination node. If any congestion found in the Network1 node, the cluster 1 will try to choose an alternate node as best node for sending the data to the valid destination. If there is any node failures or attacks present inside the router then this proposed router will try to send the data in alternate way to the destination node.

### 3. ROUTER MANAGER MODULE

In this module, Router Manager is the node which is used to measure the attacker details which is present inside the network. This router manager will try to verify the node status and its attack details and this will be identifying the energy details and find attackers. This is used to provide an alternate path if there is any attack found during the data transmission.

### 4. DESTINATION MODULE

In this module, the destination is a node which will be receiving the data from the sender via router. The destination can view the data packets in plain text manner only if all the data from sender is received successfully by the destination node. The destination node can save the received data into its buffer location which is present in that application folder.

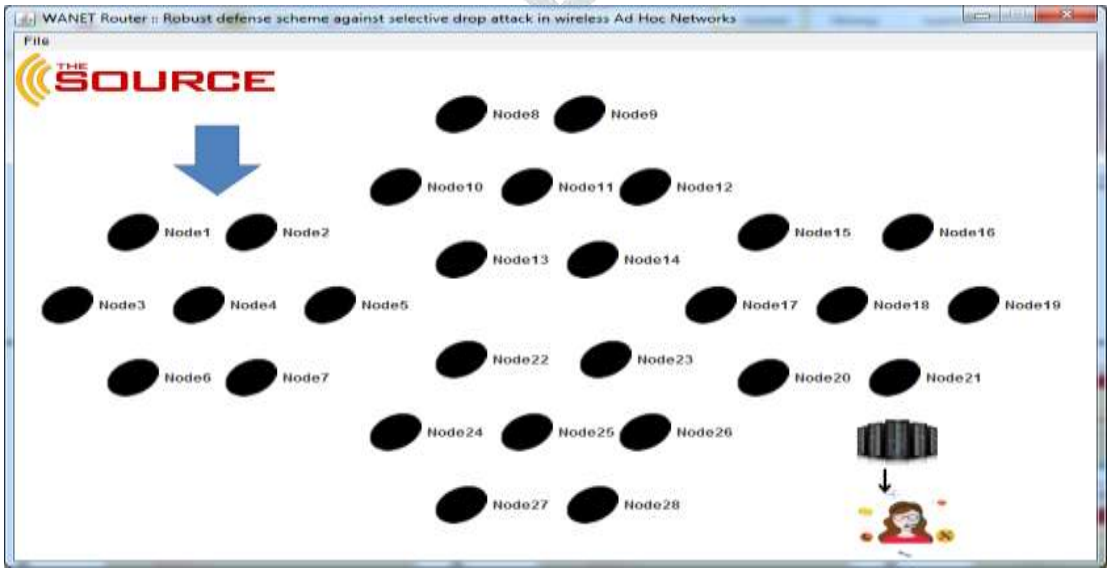
### 5. ATTACKER MODULE

In this module, attacker selects the Network and node, gets the original energy size and modifies the energy size for the node.Here we try to apply selective drop attacks by choosing the node and then try to decrease the energy levels of that node and try to morph with low energy.Once if any node is reduced in its original energy then such a node is automatically identified as attack node and this attack nodes are monitored by the router and router manager windows.

## V. EXPERIMENTAL RESULTS

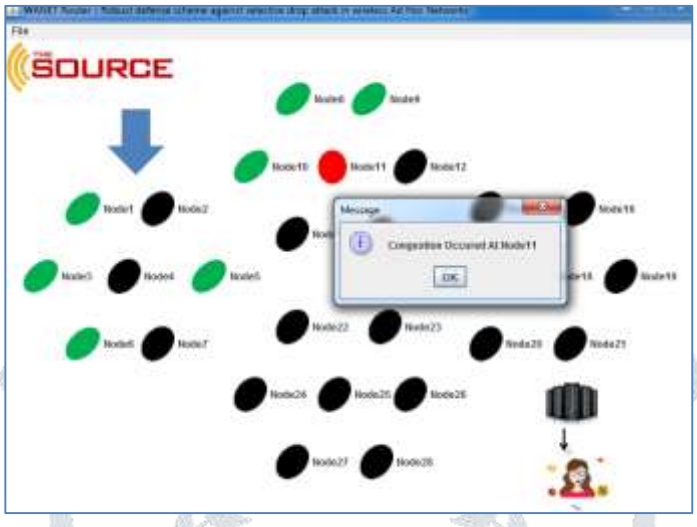
Here in this proposed application to use Java as programming language with JSE as chosen environment .The front end of the application takes AWT, Swings and Socket Programming and the back end of the application takes My-SQL database.

**WANET ROUTER WINDOW**



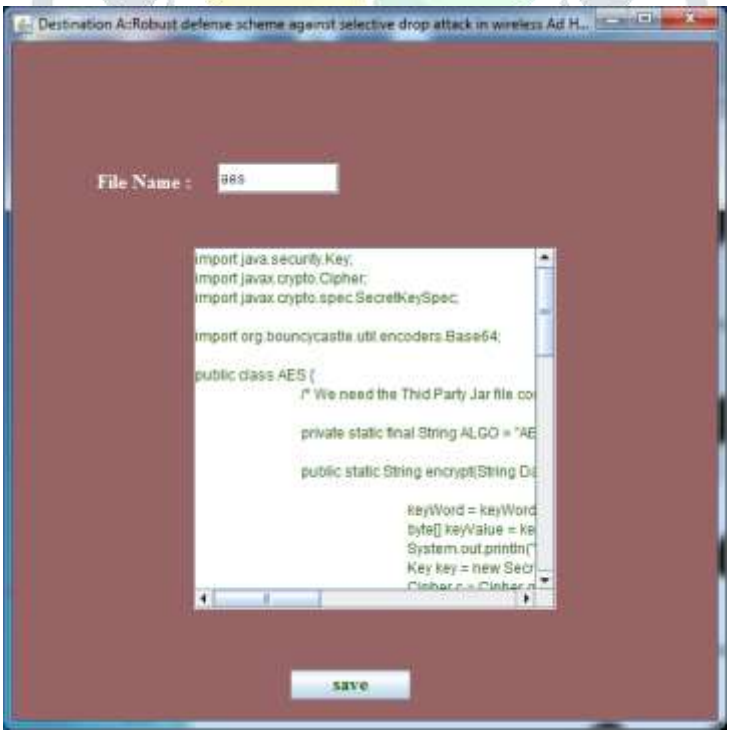
From the above window we can clearly identify that router will contain a set of intermediate nodes which acts as sensors in real time networks. Initially all the sensors need to be activated by the source node and once they are activated the router can able to find out the node capability while choosing best path.

**SOURCE NODE FINDS THE ATTACKER DETAILS**




Here the router node will try to find out the failure nodes which are present inside the router and then try to observe the attack details and then try to monitor best path s.

**RECEIVER WINDOW WILL RECEIVE THE DATA**




Here the receiver window will receive the data in plain text manner only if all the data packets are received success.if any packets are not received properly the data cannot be viewed in plain text manner.

## VI. CONCLUSION

In this proposed paper we finally came to a conclusion that we proposed a new resistive to selective drop attack (RSDA) scheme which can able to provide an effective security for selective drop attack. It is important that the illegitimate nodes should be identified which overload a host and isolate them from the network by holding its transmission process. In this proposed paper, we present a Resistive to Selective Drop Attack (RSDA) scheme which can protect the sensitive data not to be dropped or revealed by the intruders who try to hack the data during data transfer; this will be act as a protective layer which provides security against selective drop attack. This RSDA protocol will try to protect the data from the intruders who try to create any type of attacks in the network, by providing an alternate path from the Point of Attack (POA) and can able to send the data packets in alternate best path. By conducting various experiments on our proposed method, our simulation results clearly state that our proposed approach will try to provide positive data transfer and try to find out the end to end measurements like delay, throughput, overhead and energy loss.

As a future work we want to extend the same application on some more attack detection and prevention of sensitive data not to be effect on the quality of data. If we can able to design a single protocol which can detect multiple attacks and provide a counter measure for all the intrusions which are created by the intruder, we can get much more attention by several users and then we can able to send the data successfully to the destination nodes.

## VII. REFERENCES

[1] H. Wu, C. Qiao, S. De, and O. Tonguz. Integrated cell and ad hoc relaying systems: iCAR. J-SAC, 2001.

[2] Y. H. Tam, H. S. Hassanein, S. G. Akl, and R. Benkoczi. Optimal multi-hop cellular architecture for wireless communications. InProc. of LCN, 2006.

[3] Y. D. Lin and Y. C. Hsu. Multi-hop cellular: A new architecture for wireless communications. In Proc. of INFOCOM, 2000.

[4] P. K. McKinley, H. Xu, A. H. Esfahanian, and L. M. Ni. Unicastbased multicast communication in wormhole-routed direct networks.TPDS, 1992.

[5] P. T. Oliver, Dousse, and M. Hasler. Connectivity in ad hoc and hybrid networks. In Proc. of INFOCOM, 2002.

[6] Z. J. Haas, J. Deng, B. Liang, P. Papadimitratos, and S. Sajama, "Wireless ad hoc networks," *Encycl. Telecommun.*, 2002.

[7] S. Yousefi, M. S. Mousavi, and M. Fathy, "Vehicular ad hoc networks (VANETs): challenges and perspectives," in *ITS Telecommunications Proceedings, 2006 6th International Conference on*, 2006, pp. 761–766.

[8] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *IEEE Commun. Mag.*, vol. 40, no. 10, pp. 70–75, 2002.

[9] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Comput. networks*, vol. 47, no. 4, pp. 445–487, 2005.

[10] V. Balakrishnan and V. Varadharajan, "Packet drop attack: A serious threat to operational mobile ad hoc networks," in *Proceedings of the International Conference on Networks and Communication Systems (NCS 2005), Krabi*, 2005, pp. 89–95.

[11] M. Peng, W. Shi, J.-P. Corriveau, R. Pazzi, and Y. Wang, "Black hole search in computer networks: State-of-the-art, challenges and future directions," *J. Parallel Distrib. Comput,2016.*

[12] J.-M. Chang, P.-C. Tsou, I. Woungang, H.-C. Chao, and C.-F. Lai, "Defending against collaborative attacks by malicious nodes in MANETs: A cooperative bait detection approach," *IEEE Syst. J.*, vol. 9, no. 1, pp. 65–75, 2015.