Proceedings of the International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT 2023)
IEEE Xplore Part Number: CFP23CV1-ART; ISBN: 978-1-6654-7451-1

2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) | 978-1-6654-7451-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/IDCIoT56793.2023.10053547

A Novel Composite Intrusion Detection System (CIDS) for Wireless Sensor Network

Swaminathan K
Teaching Fellow / ECE Dept.
University College Of Engineering
Pattukottai, India
swaminathan.vinoth@gmail.com

Vijay Ravindran*
Assistant Professor / EEE Dept. Saranathan College Of Engineering
Trichy, India
vijay91mtech@gmail.com

Ram Prakash Ponraj
Assistant Professor / EEE Dept.
Saranathan College Of Engineering
Trichy, India
gprsahara@gmail.com

S Venkatasubramanian
Associate Professor / CSE Dept.
Saranathan College Of Engineering, Trichy, India
veeyes@saranathan.ac.in

K.S Chandrasekaran,*Associate Professor / CSE Dept.*
Saranathan College Of Engineering
Trichy, India
chandrasekaran-cse@saranathan.ac.in

Satheesh Ragunathan,
Assistant Professor / EEE Dept.
Saranathan College Of Engineering, Trichy, India
satheesh-eee@saranathan.ac.in

***Abstract*— Modern wireless technology demands the implementation of preset Sensor nodes for a structured wireless network. The network has sensor nodes for surveillance or environmental sensing, which wirelessly transmit data to a collection point. Therefore, data transfer must be protected by preventing external intrusion attacks. This will be handled by designing an effective intrusion detection system proposed as a Composite Intrusion detection system (CIDS). It is suitable for a network in heterogeneous network structure with a capable of identifying externals attacks like flooding of data's, sending unwanted data packets and changing the destination node. For routing of data packets between the nodes, minimum power utilization with changeable cluster heading method is used. The activities of sensor nodes will be monitored and a dataset is formed on the basis of the node's activity. It is known as Network Databases (NDB). Using this dataset, the intrusion attacks will be identified by using Artificial Neural Network (ANN). ANN will be trained with a predefined dataset for the effective identification of external attacks. The proposed CIDS methodology shows the high accuracy of identifying the external attacks on the sensor networks when comparing to the previous designed system in all the types of attacks.**

Keywords— ***Wireless Sensor Networks, External Threats, Intrusion, adaptive networks.***

I. INTRODUCTION

Wireless based sensors networks is a revolutionary invention in the modern era used for all types of application like surveillance in military application, collection of health-related data in medical field [1]. It has set of distribution sensor nodes in an application area for sensing the data with a predefined geographic location. The location of nodes will be decided on the basis of XY co-ordinates. The sensor nodes have to collect the sensing data from their corresponding location and passed to a cluster head. The head nodes will make effective data aggregation method and passed the concern data to base station [2]. The data transmission will be done by using any of the routing protocols and it should be secured from the external threat. Also, the power backup of the sensor is a tradeoff between the data transmission and securing the data from the threats [4]. The data packets routing is depicted in figure 1.

As the sensor nodes are in open area and the data transmission will be carried over in an open platform with limited network resources, the chances on injection of threats will be high. In spite the position of nodes is a heterogeneous network, chances on threats will be high [5].

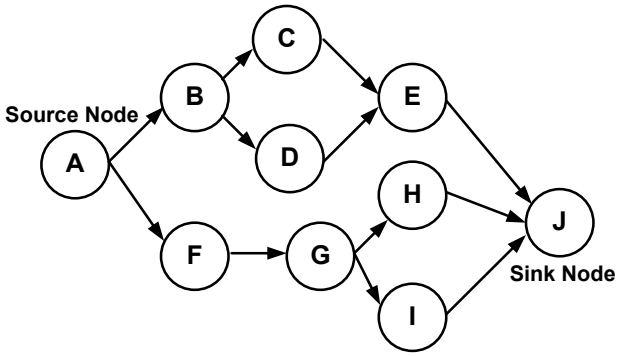

Fig. 1. Routing of data packets between nodes in a network.

The external network attacking people will take over the control of sensor nodes and placed some of unwanted data packets. The packets will get transmitting on the network creating a vulnerable for the privacy of data transmission. There are many types of threats over the network. But the important objective of the threats is to inject a unwanted data packets and makes the network resources to get wasted. This will result in the nodes to enter into a dead condition and the entire network will get into an inactive state. [6-8].

As the head of the cluster (CH) is point of data collection or data aggregation, the chance of external threat for the heading nodes is maximum. External threat is a degradation attack by any network engineer to enter into a network structure [9]. Defining a methodology for identifying the external threats is difficult because this node will have limited amount of power back up and supporting hardware components [10]. A network structure which has a heading node is shown in figure 2.

Authorized licensed use limited to: Carleton University. Downloaded on June 15,2023 at 06:42:38 UTC from IEEE Xplore. Restrictions apply.

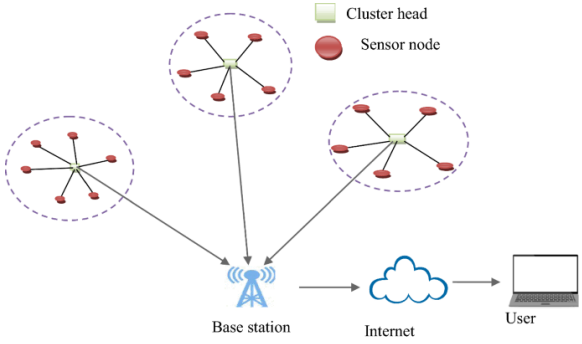

Fig. 2. Network structure on the basis of Cluster head

In this research work, the external threat is identified by implementing an effective ANN in the network strategy and identifying the type of attacks also. This is done by training the ANN with a data set of normal activities of the sensor nodes. This will help the neural network for identifying the external attacks. The database is collected by the heading nodes from the time of implementation of nodes in a network itself. Hence, external threats will be identified in an effective manner. For the routing of data packets, a low power consumption adaptable clustering protocol is used. The flow of the research work is formulated as section 2 discusses about the background of the proposed methodology, section 3 and 4 discuss about the proposed CIDS methodology, experimental results and discussion respectively. The section 5 and section 6 explain the conclusion of the proposed system and the references used for proposed system.

II. BACKGROUND OF THE PROPOSED WORK

This section will discuss about the Low power consumption routing methodology, Adaptable data packet transmission, external threat identifying system.

A. Low power consumption routing methodology:

In this type of routing strategy, the network is setup with predefined density of nodes in a sensor network. This count on nodes is depending on coverage capacity of each node. Hence each node is designed to have a maximum coverage. This is for minimizing usage of sensor nodes in a network structure [11-13]. Also, it will be a well-defined network link for effective way of communicating between either between neighbor nodes or directly to a base station. The entire structure of network is subdivided into separate groups of nodes under a heading node (HN). The heading node is a (like a supervisory node) commanding point of all the sensor nodes in a group. It also collects the data from all of its group nodes and makes an effective data aggregation process with the external a base station. It has two phase of process one is setting up of network and other one is Data transmission state.

In the first phase the nodes will be grouped in accordance with the energy, distance and all other basic network parameters. After setting up of the network, the network startup message will be passed for the confirmation of neighbor nodes. In the second phase of the routing the data transmission will be carried over the sensor nodes in predefined routing path. The path is selected and intimate by the routing protocols used

B. Adaptable data transmission.

Here we use lower energy usage for the data transmission as the sensor nodes has a limited amount of power backup and it is difficult to retain power resources of the sensor nodes. The data transmission will be initiated only when the residual power backup, distance between the nodes and other basic network metrics to be collected by the Heading node (HN). [13-18].

After the data set is formed it will be formulated as a network metrics table by all of the sensor nodes in a group. The heading node will make effective path identifying process for the successful data transmission between the source and destination point. If the data path is decided, it will be intimated to all other nodes of a group. This is for making the path identification between source and destination node. Finally, the data transmission will be initiated and the packet transmission is monitored by the heading node (HN).

If there is any of the nodes get into in-active stage. The data path will be changed over to an alternative data path by the heading node (HN). On this occasion the heading node will give a standing control over the group of nodes for not making of any data transmission. The data transmission is continuing in alternative path from the stage where it gets paused in the network.

C. External threat identifying system:

In the sensor nodes implementation in a wireless manner, the data transmission will take place in an open manner. It implies the data transmission path, source and destination nodes are explicitly known to all other part of the network. The chances of attack from the external network are high. Also, it is difficult to identify the attacks in between a data transmission. This is because of injection of unwanted data packets in the middle part of the data transmission process.

Also, the threat may occur by changing of the data path in wrong manner. This will create a network overhead in data path during a packet transmission [14]. For this an effective way of identifying the alternative data path in a short span of time will decrease the network resources to be wasted in the flooding of data packets in a wrong data path, it will happen mostly in a long duration of data packets between a set of nodes. For a short duration of packet transmission, network attackers will not have anytime identifying the data path, source and destination node addresses [15].

Sometimes threat will create a wrong identification on destination node location. This will create a headache on identifying the shortest data path. At this stage, heading node (HN) will take much more time duration for the confirmation of source and destination node addresses. Then it will decide the shortest data path. The two most significant functions of CIDS methodology proposed are. ,

Network features collection: In the phase, networks basic metrics related on the identification of external threats to the network. The data will be formed as a network database (NDB).

Formation of algorithm: Here the methodology will formulate the flow for identification of threats and types of the threats. The efficiency, accuracy on the detection of threats is noted down from this phase.

The flow of the identification of threat and its type is shown in the Figure 3. The components of flow chart is explained as

Deployment of network: Here the nodes will be deployed in a predefined position on the basis of coverage capacity of sensor nodes.

Authorized licensed use limited to: Carleton University. Downloaded on June 15,2023 at 06:42:38 UTC from IEEE Xplore. Restrictions apply.

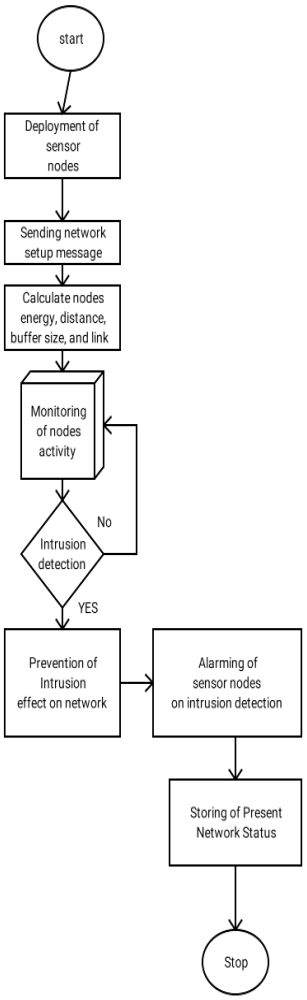

Fig. 3. Flowchart of CIDS methodology

Setup Message: This is a startup message issued by the heading node to all of the sensor nodes in a group for confirmation node's activity.

Calculation of distance, energy: The basic network metrics will be calculated between the sensor nodes and it is maintained as a network metrics table.

Monitoring of Nodes: The node's data transmission and other activities will be investigated periodically.

Alarming to nodes: When there is threats are identified, other nodes will be intimated for storing the current network status.

Storing of current status: the network basic parameters will be stored for the future use after threat detected.

III. PROPOSED TOPOLOGY

The proposed various ideology for determining the external threats and types of threats in the network.

A. Flooding of Data

This type of threats will happen when the network attackers inject the unwanted data in the network data paths and it is transmitted in the destination side. All the data packets will have source node ID followed by data packets. But unwanted data packets will not have proper source ID. Hence on investigating the source ID number in the receiver side, we may conclude the data packets having mismatch of source ID is the unwanted data packets. The flow of algorithm is shown in *Algorithm 1*

Algorithm 1: Data flooding in Network

$n \rightarrow$Network Size

$S_N \rightarrow$Sensor Node, $M_N \rightarrow$Malicious Node

$C_H \rightarrow$Cluster Head, $B_S \rightarrow$Base Station

$C_M \rightarrow$Cluster Member, $N_C \rightarrow$Cluster Heads list

$x \rightarrow$Integer value between 0 and $N-1$

$S_N i$, $0 < i \leq N$, compute ($S_N i$) and random$rS_N i$

IF ($rSNi < (S_N i)$) THEN

$S_N i = C_H$

ELSE

$S_N i = CM$

ENDIF

$C_H j$, $j \in N_C$

{

$C_H j$ broadcasts the advertisement message (ADV CH)

x C_M will join $C_H j$

$C_H j$ creates TDMA schedule

x C_M send data to $C_H j$ in the corresponding TDMA time slot

}

IF $C_H j$=MN THEN

Performs the attack by dropping all packets

ELSE

Sends aggregated data to B_S

END

The above algorithm shows the data flooding threats, data in a network initially the data will start to transmitted and heading node will start to monitor. On the transmission of data packets, each packet will be compared by the training dataset stored in the neural networks for the identification of external threats. A trained data is one which has proper ID structured of the sensor nodes in the network structure and also has the prescribed data packet size. Whenever the threats detected by identifying the unwanted data packets, it will be intimated to all other nodes for storing the current status. This is to restore the network back to the normal condition after removing of threats in the network structure.

In the network structure, in a abnormal condition data packets will flow to recover the network to be in normal conditions. The data packets are termed as Control packets. The process of network recovery from abnormal condition will checked periodically and the process is known as Routing Overhead

B. Sending unwanted Data Packets

Transmitted of unwanted data will wasted the networks resources. Hence it should be avoided the proposed methodology will effectively identify this type of threats. The flow of the algorithm used for this type of threats is shown in Algorithm 2.

Authorized licensed use limited to: Carleton University. Downloaded on June 15,2023 at 06:42:38 UTC from IEEE Xplore. Restrictions apply.

Algorithm 2: Injection of unwanted data in data path

$n \rightarrow$Network Size

$S_N \rightarrow$Sensor Node, $M_N \rightarrow$Malicious Node

$C_H \rightarrow$Cluster Head, $B_S \rightarrow$Base Station

$C_M \rightarrow$Cluster Member, $N_C \rightarrow$Cluster Heads list

$x \rightarrow$Integer value between 0 and $N-1$

$S_N i, 0 < i \leq N$, compute $T(S_N i)$ and random $rS_N i$

IF $(rS_N i < (S_N i))$ THEN

$S_N i = C_H$

ELSE

$S_N i = C_M$

ENDIF

$C_H j, j \in N_C$

{

$C_H j$ broadcasts the advertisement message (ADV CH)

x C_Ms will join $C_H j$

$C_H j$ creates TDMA schedule

x CMs send data to $C_H j$ in the corresponding TDMA time slot

}

IF $C_H = M_N$ THEN

Performs the attack by dropping some packets (randomly or selectively)

ELSE

Sends aggregated data to B_S

ENDIF

Using the specified Algorithm 2 the unwanted data packets are avoided in a effective way using TDMA methodology for checking of the data's in periodically. Generally, TDMA methodology is used to find any unwanted data packets. This is because of data packets will be forwarded in network in stipulated time scale only. If any data packets hopped in the network on a different time scale, then it will be categorized as unwanted data packets. In this proposed work, for specified time interval the format data packets are checked with training dataset. If there are any changes it will be identified as threat to the network architecture. Then the threat will be removed to restore the network in normal condition.

IV. RESULTS AND DISCUSSION

In the experimental methodology, the implementation will be conducted in a network simulator with link-layer protocol, the IEEE standard of 802.11 Mac protocol. In the simulation environment, the network is deployed in 1200 × 1200 m2, respectively. The network setup is deployed randomly in which the nodes are free to navigate anywhere but within the range. The total number of nodes taken for the experiment is 100 randomly deployed using a random mobility model. The communication is established from the source node to the destination node. The multicast constant bit ratio is used for examining the network traffic, and the range of node mobility is 10-20 m/s. The packets with size 2000 bytes are taken for communication and the data connections are established using TCP or UDP. The below table I illustrates parameters of the proposed research work.

TABLE I. PARAMETERS OF THE PROPOSED RESEARCH WORK

Simulation Parameter	*Value*
Simulator	NS-2
Simulation time	150 s
Number of nodes	100
Simulation area	1200 × 1200 m2
Mac Protocol.	IEEE 802.11
Data rate	12 Mbps
Radio range	100m
Mobility model	Random waypoint model
Antenna	Omnidirectional Antenna
Packet size	512 bytes

A. Transmission delay comparison.

The graphical representation shown in Figure 4, shows end-to-end transmission delay results of algorithm used concerning the total number of nodes with a comparison on table II. The time delay is manipulated by the relation $1/(x\text{-}y)$ where x is the count of data packets/second the facility and y is the average rate at which packets are arriving at the destination node. The delay metrics should be minimal because on identification of threats. If there is any delay threat will spread to entire network structure. Hence, proposed CIDS methodology achieves minimum delay on comparison with other related works.

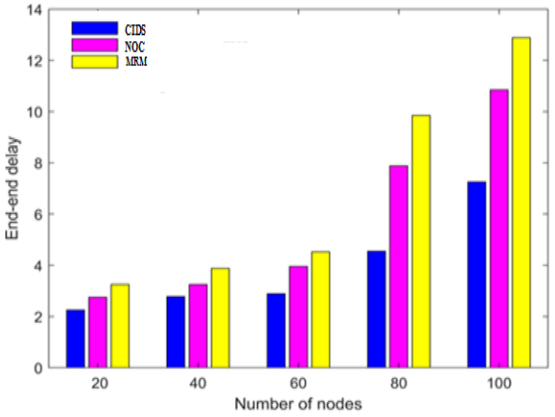

Fig. 4. Count of nodes vs. end-end delay

TABLE II. DENSITY OF NODES VS. END TO END TRANSMISSION DELAY

Count of nodes	CIDS(ms)	NOC(ms)	MRM(ms)
20	2.36	2.45	3.2
40	2.88	3.35	3.68
60	2.94	3.85	4.42
80	4.75	7.8	9.65
100	7.55	10.65	12.8

B. Delay of various system

In WSN, data from sensor nodes will be managed without delay in the transmission and identification of threats in the senor network. This will be accomplished by giving proper trained set to neural network for separating normal data packets and threat initiated data packets to sink without

Authorized licensed use limited to: Carleton University. Downloaded on June 15,2023 at 06:42:38 UTC from IEEE Xplore. Restrictions apply.

any delay in the transmission process. From figure 5, we may see the proposed algorithm has a minimum delay in comparison with all predefined methodology on identification and separation of normal activity and threat affected activity. It is formulated by making the availability of multipath transmission in network.

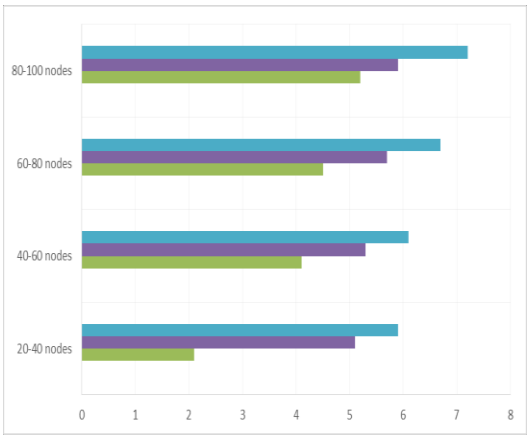

Fig. 5. Identification of delay in threats

C. *Total Execution Time*

The total execution time of various methodologies is shown in figure 6. In the graphical representation number of task is increased for various methods simultaneously. But the proposed method CIDS has a minimum execution time even for performing 250 tasks while other existing systems are utilising maximum time for their execution. If any threat detected means execution time includes identification of threats, alarming of other nodes in the network structure and storing of current status of network transmission cycles. But in normal network working condition it is a time for which all data packets reached the destination node for a given network load.

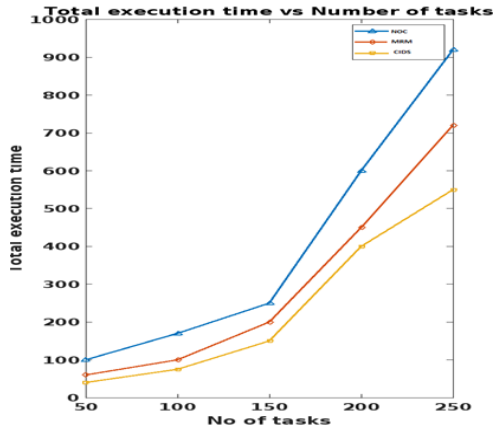

Fig. 6. Overall execution time of various systems

V. CONCLUSION

The fundamental purpose of the CIDS is to identify external threats and their nature before they penetrate the network's structure. As a result of the excellent implementation of data packet routing, detection is performed efficiently with the aid of a changing cluster heading node and low power consumption of sensor nodes. As the CIDS identify risks utilizing artificial neural networks, its efficiency is superior to that of existing specified research networks. The sort of external attacks recognized by the planned CIDS flooding of Data's unscheduled data transmission is a significant factor. This is because data flooding reduces network efficiency and causes a significant amount of network resources to be squandered. By providing the correct data set during the training phase of neural networks, this threat detection can be modified. This is done on a periodic basis to acquire the node activity dataset. Therefore, the suggested system is capable of identifying external threats and their categories in the shortest time possible, with advance notification to all other networks on the sorts of threats found.

REFERENCES

1. A. Braman and G. R. Umapathi, "A comparative study on advances in LEACH Routing protocol for wireless sensor networks: a survey," International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, no. 2, pp. 5883–5890, 2014.
2. H. Dhawan and S. Waraich, "A comparative study on LEACH routing protocol and its variants in wireless sensor networks: a survey," International Journal of Computer Applications, vol. 95, no. 8, pp. 21–27, 2014.
3. D. Kumar, "Performance analysis of energy efficient clustering protocols for maximizing lifetime of wireless sensor networks," IET Wireless Sensor Systems, vol. 4, no. 1, pp. 9–16, 2014.
4. Y.M.Miao, "Cluster-head election algorithm for wireless sensor networks based on LEACH protocol," Applied Mechanics and Materials, vol. 738-739, pp. 19–22, 2015.
5. Vijay Ravindran, Vennila C "An energy efficient clustering protocol for IoT wireless sensor networks based on Cluster supervisor management" Comptes rendus de l'Acade'mie bulgare des Sciences, December,2021.
6. V. Ravindran, R. Ponraj, C. Krishnakumar, S. Ragunathan, V. Ramkumar and K. Swaminathan, "IoT-Based Smart Transformer Monitoring System with Raspberry Pi," 2021 Innovations in Power and Advanced Computing Technologies (i-PACT), 2021, pp. 1-7, doi: 10.1109/i-PACT52855.2021.9696779.IEEE
7. Ravindran, V. and Vennila, C., Energy consumption in cluster communication using mcsbch approach in WSN. *Journal of Intelligent & Fuzzy Systems*, (Preprint), pp.1-11.
8. Swaminathan, K., Ravindran, V., Ram Prakash, P. and Satheesh, R., 2022. A Perceptive Node Transposition and Network Reformation in Wireless Sensor Network. In *International Conference on Computing in Engineering & Technology* (pp. 623-634). Springer, Singapore.
9. Vijay, R., Madhuranthagi, T., Dhurga Devi, A. and Kanimozhi, S.A., 2020. July. IoT Based Smart Vehicle with over-Speed Accident Detection and Rescue System. *International Journal of Advanced Science and Technology*, *29*(9), pp.3297-3304.
10. Swaminathan, K., Ravindran, V., Ponraj, R. and Satheesh, R., 2022. A Smart Energy Optimization and Collision Avoidance Routing Strategy for IoT Systems in the WSN Domain. In *International Conference on Computing in Engineering & Technology* (pp. 655-663). Springer, Singapore.
11. S.venkatasubramanian, "Correlation Distance Based Greedy Perimeter Stateless Routing Algorithm for Wireless Sensor Networks", Int. J. Advanced Networking and Applications Volume: 13 Issue: 03 pp. 4962-4970,2021.
12. S. Venkatasubramanian, D. A. Suhasini, and D. C.Vennila, "An Energy Efficient Clustering Algorithm in Mobile Adhoc Network Using Ticket Id Based Clustering Manager," International Journal of Computer Science and Network Security, vol. 21, no. 7, pp. 341–349, Jul. 2021.
13. Venkatasubramanian, S., Suhasini, A. and Vennila, C., "An Efficient Route Optimization Using Ticket-ID Based Routing Management System (T-ID BRM)". Wireless Personal Communications, pp.1-20, 2021
14. S. Venkatasubramanian, A. Suhasini, C. Vennila, "Efficient Multipath Zone-Based Routing in MANET Using (TID-ZMGR) Ticked-ID Based Zone Manager", International Journal of Computer Networks and Applications (IJCNA), 8(4), PP: 435- 443, 2021, DOI: 10.22247/ijcna/2021/209709.
15. Srinivasan, Venkatasubramanian, "Detection of black hole attack using honeypot agent-based scheme with deep learning technique on

Authorized licensed use limited to: Carleton University. Downloaded on June 15,2023 at 06:42:38 UTC from IEEE Xplore. Restrictions apply.

MANET", Ingénierie des Systèmes d'Information, Vol. 26, No. 6, pp. 549-557.2021.https://doi.org/10.18280/isi.260605.

Authorized licensed use limited to: Carleton University. Downloaded on June 15,2023 at 06:42:38 UTC from IEEE Xplore. Restrictions apply.