International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Reliability Assessment and Detection of Nodes Causing a Blackhole Attack in Portable Informal Networks

S. Murali[1*], V. Sathya[2]

Submitted: 10/10/2023 **Revised**: 29/11/2023 **Accepted**: 10/12/2023

Abstract: In mobile ad hoc networks (MANETs), the existence of malicious nodes might raise serious security issues. These nodes could interfere with the routing procedure or change the way data packets move through the network. Due to the entire framework's traits including its lack of structures, changeable topology, and central management unit, the MANET is very vulnerable to attacks. The black hole attack is one of the most frequent in MANETs, which In the event of such assaults, MANET nodes are vulnerable to a remarkable network capacity reduction. with this aspect, it is difficult with MANETs to identify or stop dishonest nodes from launching blackhole attacks. A decentralized anomaly detection system called identifying intrusions using traffic projections, which is based on this method, is created for detecting attacks that have a greater impact during packets moving, like selectively attacks with DOS or relaying strikes. Each node in TPID operates separately when anticipating volume and spotting anomalies. It is not necessary for nodes to cooperate or use specialized hardware. In experiments, the plan is assessed and contrasted with alternative methods. Results demonstrate that the suggested technique achieves a high detection efficiency with little extra cost for computation or communication. In this research, we provide an Enhanced Blackhole Resistance (EBR) mechanism to recognize and thwart blackhole attack-causing nodes. By sending the data packets through an encrypted route with the smallest RTT, EBR can avoid clogged traffic. The EBR protocol employs a TR mechanism, often known as a duration to live and time spent traveling combined, to identify blackhole assaults. No authentication or cryptographic techniques are needed for our algorithm. Compared to other protocols, EBR performs better in simulations in terms of efficiency, end-to-end delay, the delivery of packets ratio, energy use, and routing inefficiency.

Keywords: *Wireless, MANET, Blackhole, attack, Routing, Round trip Time, Time to live, Congestion*

1. Introduction

A MANET is a wirelessly connected, self-configuring system of dynamic nodes. Every node has complete freedom of movement and can function as a router or host. By sending packets through intermediary nodes to the end nodes, data communication is accomplished. For communication in MANETs, a variety of routing protocols have been developed [1]. When contrasted with single-route mechanisms like Ad-hoc Upon request The length Vector (AODV), AOMDV is more effective, especially when nodes move around and more data is lost [2]. However, due to their ease of mobility and lack of infrastructure, networks are vulnerable to safety concerns and assaults. The performance of the network is significantly decreased by a blackhole assault, sometimes referred to as a container-dropping attack [5]. Blackhole assaults often fall into one of two categories: single a black hole node or many blackhole nodes. It is known as a coordinated black hole attack when numerous blackhole nodes work together to disrupt communication encrypted methods [6].

On the other side, various confidence models and trust systems have been put forth. This is done to improve security in MANETs because nodes can directly or indirectly gain a neighbor's trust through endorsements from other nodes. However, the blackhole node [6] promptly sends back an RREP after receiving an RREQ packet with the false claim that it has the shortest path to the recipient's side and a very large sequence number. The path's recentness is shown by the high sequence number. The data packet will be lost if the node that sent it chooses a route with one or more blackhole nodes. The prevention of blackhole assaults has been suggested for a number of reasons. Existing protocols have security additions, and the packets have nodes. There are multiple states security measures, such those in [7]. Although computationally intensive, cryptographic mechanisms may perform worse than less secure alternatives if attackers are present. Giving the routing packets a secure protection does not guarantee that the dodgy nodes will be found. This inspired us to create a technique that securely vaults data packets, consumes less energy, and improves the performance of the standard of service (QoS) [8].

In this paper, we introduce the Expanding Blackhole Restriction (EBR) method that can identify routes with unwanted nodes in cellular networks and, as a result, stop or significantly decrease the data packets travelling via those routes. EBR is useful for any reactive technique. We employ EBR in this case together with the AOMDV method to determine the optimal routes since it performs best when

[1]*Assistant Professor, Department of computer science, MGR College, Hosur 635109, Tamil Nadu, India*
.Email:murali.research2016@gmail.com
[2]*Assistant Professor, Department of computer science, MGR College, Hosur 635109,Tamil Nadu, India. Email: sathyanakar@gmail.com*

combined with a multiple path routing protocol in selecting the route that enhances the quality of data delivery. Each node evaluates nearby ones and provides trust values to them in order find the a blackhole nodes. This approach provides protection versus both solitary and collective attacks, and it operates far better than earlier protocols. Reported TR algorithm having an EBR protocol built on top of it, based on TTL and RTT. EBR raises the efficiency of networks. Blackhole assailant(s) in the spread pathway and information bottleneck at protuberances in between in a communication path; the capacity to filter out pathways provided by AOMDV to circumvent a blackhole aggressors and overfilled sites. Correspondence our EBR protocol against various evaluation methods through simulation. An overview of the organization of this essay can be found below: In Section 2, a review of the literature is given. The proposed protocol along with methodology is presented in Section 3. Section 4 presents the model's findings and the complex nature of the protocol. Section 5 lists all of the conclusions.

2. Review of Literature

The two primary categories of network security solutions are prevention-based strategies and detection-based techniques [11]. The deceptive attacks established by outside attackers can be stopped by attack prevention mechanisms that involve authentication, handling keys, security, routing protocols, and others, but it is challenging to counteract assaults, which are more effective at obscuring and destroying information and difficult to defend against when false incidents are initiated by taken nodes. Through identification and avoidance processes these kinds of assaults must be addressed. The current WSN intrusion detection schemes evaluate intrusion primarily with the analysis of data or flow parameters along with cooperation among nodes, placing high demands on the nodes' computational and storage resources [12]. Additionally, extra costs related to communication will swiftly deplete the nodes' limited energy. Therefore, a crucial problem to be resolved is how to reduce resource costs as quickly as possible while still offering an improved detection rate.

The goal of the research presented in this article is to develop a network regarding the substantial paved WSN. TPIDS will be used to identify attacks like selective transmitting attempts and denial-of-service attacks that have a significant impact on the flow of traffic. This is the very first intrusion detection system for WSN that uses the traffic forecasting approach that we are aware of, both domestically and internationally [13]. These two points are the article's key contributions. The technique does not call for additional hardware assistance or node coordination. The updated Markov model provides a high degree of prediction accuracy, according to simulation findings. When compared to intrusion detection systems based on cooperation, TPIDS constitutes a lightweight an invasion detection scheme with extremely low overhead that can be used to detect intrusion behavior more quickly while using less energy and communications. The assault packets are anticipated to be noticeably different in energy and speed from the typical message in the proposed distributed cooperation anomaly detection technique. The engine radios alert information when abnormality is found [15]. If an alert message that node A had gathered against node B reached the predetermined dawn, node A was certain that node B proved to be the intrusive node. The following two points are the scheme's drawbacks. First, consider the intensity and accelerate of the assault's information have a direct impact on the detection rate; when the attacker sends the message with energy and speed that are similar to normal to avoid being identified, the probability of detection is significantly decreased [16]. The restricted electrical power of nodes and the constrained network bandwidth will be swiftly depleted as a result of nodes cooperating to determine the anomalous, lowering the network's lifespan. An anomaly detection method was used to find a routing assault on Loo. The node will then appear in the sparse part of the feature space during the test stage if the characteristics knowledge extracted [17] from the packet stream is present. This system allows for nodes to independently detect anomalies, which lowers communication costs. However, the training process requires the collection of twelve unique network traffic traits as well as computation of the average and modification for every attribute, increasing the difficulty of the system's estimates. A popular reactive protocol is AODV. According to [18], it poses a serious security risk to routing protocols, putting the blackhole node at risk. [19] came to the conclusion that AODV performs poorly when the chosen route contains blackhole nodes. Additionally, it was demonstrated experimentally in some cases that the AODV protocol's performance degraded when a blackhole attack occurs. To decrease the likelihood of having a wicked or single-blackhole node, [20] modified the AODV method. However, when two cunning attackers work together to launch the attack, this mechanism is vulnerable to cooperative blackhole threats.

The additional routing overhead cost added by this message increases nodes' energy consumption. The Cooperative Bait Detection Scheme (CBDS), a blackhole detection technique, was put forth in [21]. PDR could decline for any other cause, such as traffic issues; nonetheless, our approach will take harmful nodes into account when determining why [22].

To lower the cost of contact and the estimation wastage of the node that is sinking, [6] presented an approach for detecting versus a similarly ordered WSN. The sink component serves as a base in an architecture constructed around a network, whereas the main node is commonly chosen. When a time period ends, the network's node

locations split. Each branching node collects cyclical flow of statistics-collecting characteristics data into identical subsets at one particular location and send the packets data to a parent node, which combines all sub-node packets to send to the next level. Up to the pump node, that displays all groups and scans for anomalies, this iterative process is repeated. Apex nodes, or nodes that undertake advanced analyses of data, simulation, and bad decision-making, will get the information that's provided to them from low-end nodes. [15] proposed a Wireless Sensor Network (WSN) anomaly detection technique based on buried Markov models, with a placement of only a handful of in the network, but much higher electricity and resource use in the high-end nodes. Ren provides a assault detection and defense solution using information from the link layer whilst taking account of the interface standard security issue technique.

3. Methodology of the work

3.1. Proposed Protocol

In order to identify black hole assaults in MANETs, the KNN clustering technique along with fuzzy predictions will be used in this study. Figure 3 shows the general design of the proposed method (Algorithm 1). This system can identify attacks thanks to the knowledge the nodes provide. For this reason, the nodes keep an eye on the sent packets. Then, using KNN the case of clustering the nodes' friends are identified.

Algorithm 1

Input: source routes

Output: source route Security measures start

Select a route randomly;

Few networks should be placed around the route;

Compute routingprotocols of the route by two nearby routes;

ID= R1(ID) +R2(ID);

Find the route with the greatest ID; Claim the assault's to be the route;

End;

Clusters are formed from all the nodes that are contained within a given range. Each node evaluates its level of confidence in the neighboring nodes and interacts with them in accordance with these values. The cluster head can therefore be suggested as the node within every cluster whose value is greater than a certain threshold [22-24]. Fuzzy deduction from the prospective nodes is then used to select the cluster leader, which is a possible node with the most reliable friends at the right amount of energy. When the network is established and the clusters are identified, cluster executives and nodes will have a mutual confidence. Unwanted nodes will then be found and the network will start employing closed routing. The definition of fuzzy logic rules must, on the one hand, avoid adding to the system's complexity. On the other hand, it raises the system's assault detection accuracy. As seen in Figure 4, if another node enters the group, Algorithm 2 is notified and given the confidence it deserves.

After receiving the RREQ document, it's possible that the attacker node will send out a method reply (RREP) packet and declare that it has the shortest path. This risky course of action is usually taken by the sender, who sends data packets by the server or nodes of a black hole, which would subsequently discard those packets. Moving through such attack node(s) affects the routing's energy use, speed, and overhead in addition to the route security issue.

3.2. The Suggested Repair

To recognize and avoid blackhole nodes in mobile networks, we offer an Advanced Blackhole Resilience algorithm. Each node examines its neighbors and evaluates its level of trust in order to identify the blackhole nodes. The improved blackhole defense mechanism provides protection from both solitary or collective attacks. Expiration ought to be set to a low value to limit its scope to nodes close by and prevent overloading the system with traffic. In general, the RTT function suggests that even though the travel path is safe, the route extremities should be ignored since they may be congested. With this technique, a brand-new idea known as more blackhole disagreement is introduced, which both locates and eliminates the black holes node. By preserving successful journey times, they add a small modification to the original adaptive procedures. Every node in a network must evaluate the performance of the nodes around it to see if any, like blackholes or overloaded nodes, are acting dishonestly.

Following is a list of the main elements of the power source EBR protocol using our TR process in Figure 1:

• Tests for route requests: Periodically, every node in the system transmits sending an exercise message to a phony node that is the destination. The examined message's time to live has a value that is independent of n. Expanding n would result in more nodes being reviewed, giving the source node a greater understanding of the harmful nodes along a particular path. This big n must be avoided because it would add excessive overhead traffic to the network.

• Trust Levels: As suggested in Algorithm 1, there are two different sorts of trust levels: TRUST and THREAT. A entirely novel network's assurance rating is set to +1 and its confidence level with is set to 1, meaning it is trusted as a good network when it joins the network. When a node

responds to a Test_ RREQ communication, its trust level changes to THREAT. The procedures in Algorithm 2 ought to be followed in this case;

There are two more types of levels of confidence available if the node is marked as a THREAT: negative and zero. A node grants itself one degree of confidence when it believes that its neighbor is a black hole node. Nevertheless, if a nearby neighbor is thought to be the casualty of a blackhole node, its level of assurance drops to zero. To do this, we employ the many possibilities indicated below together with our TR system. Algorithms 1 and 2 are both a part of the TR mechanism. Instantaneous RTT is abbreviated as RTTi, and average RTT as RTTa. TTL may be equal to n.

When RTTiRTTa and TTL consider is low, we can use the RREP message to pinpoint exactly where the blackhole node(s) are located. If n = 1, the blackhole node is the nearby node. Given that the surrounding node is most certainly the if n = 2, it is prey of the blackhole node adjacent to it, the confidence is set to zero for that node. More prospective nodes that behave erroneously along the current route would be indicated by an increase in n;

If RTTi, RTTa, and TTL have excessive values: The node that provided the source recognizes therefore subject to the number of n, the road might contain a few a blackhole nodes, along with the fact that any of these node might be far removed from the original node. Fortunately, it is impossible to pinpoint the precise location of the blackhole node(s). When routing the data packets, this route should be avoided. The nearby node's confidence level remains unchanged. Additionally, the nearby node is uncongested and can be safely used in other paths because of this;

Since the farther node(s) are likely to be a blackhole nodes, the node at the source can infer that the nearby node(s) are likely congested. The surrounding node, which is crowded yet secure, can be taken into account in any other path. This is only acceptable if additional routes through one of these blackhole attackers are dubious; RTTi>RTTa when TTL value is high. The blackhole attacker is situated some distance from the origin node. Because of several crowded nodes or because n has a high value, the entire avoiding this route. As depicted in Algorithm 3, EBR combines our TR algorithm and a reactive routing protocol. During the testing phase, the chosen routes should take into account the confidence levels computed using our TR approach. The source node will only take into account routes that have positive confidence levels and are also less crowded when it needs to communicate. A node with zero confidence has a blackhole attacker right next to it. A low level of confidence suggests that this node is a blackhole.

[9] recommended using the detection point as a basis. Each incident packet-based is going to have a the identification indicate that generates a verification packet, the packet being stated to the upward transmission, the spread paths, as well as if the given package is not effectively recognized by an intermediary node, then advising details about abnormal packet loss that will be shown if the store is not adequately noticed by a middle node. Were chosen at random for testing so that the opponent couldn't anticipate the subsequent point of your choosing to maintain the work just takes into account choosing propagation brutality, while spreading of comprehension packages and announcements decoded on expanding, the creation of a larger conversation, and calculating costs prevent a node from becoming an aspect of the antagonist's capture with significant durability.

With the help of this approach, MANET node certification, medium access control, and secure transmission issues are resolved. SUPERMAN combines security and navigation. In contrast to other protocols, it has a high overhead, especially as the number of nodes rises. The authors of [24] suggested a protocol that uses feedback from the source node to the destination or intermediary nodes, such as ACK messages. This is done to keep track of whether the nearby nodes are trustworthy or malicious. This strategy is difficult and even doesn't substantially enhance performance. To distinguish between trustworthy nodes and malicious ones, this technique added a pre-RREP message. This is a general method for finding intrusions. In the presence of many collaborative blackhole nodes, this system probably collapses. To lessen the blackhole assault, the authors of [3] offered an improved AODV protocol. Due to the self-organizing and random nature of sensor nodes, securing Wireless Sensor Networks (WSN) has become a more difficult task in recent years.Due to its advantages of self-organizing nature, low power consumption, and reduced cost consumption, Wireless Sensor Networks (WSNs) have grown more popular[25]. This WSN (Wireless Sensor Network) is increasingly overtaking other technologies in use in commercial and industrial applications due to considerable improvements in processor, communication, and low-power utilisation of embedded computer systems[26]. For a wireless Mobile Ad-Hoc network (MANET) to operate at high data rates, efficient packet access must be improved. Due to similar traits with trustworthy nodes in the sensing region, reducing the severity will be a challenging task because the deterioration is brought on by the discovery of malicious nodes[27]. IoT is one of the upcoming internet technologies that focuses on the delivery of services and adjusting the way that technologies are implemented across various communication networks[28]. The Internet of Things (IoT), an emerging technology, makes it easy and advantageous to share data with additional devices across wireless networks. However, due of their continual development and technological advancements, IoT systems are more vulnerable to cyberattacks, which could result in strong assaults[29]. Low price, small size, and excellent energy

effectiveness The internet of things (IoT) paradigm's success depends on VLSI design. One of the main methods for achieving great performance and energy efficiency in applications that require a lot of error-resistant computation is approximate computing[30].

There are some situations in algorithm 2 where their confidence levels remain unchanged. Since each node is required to perform the integrity test on a regular basis, For nodes that are near the node that provided the data, a level of trust will be established. In other words, test node N is further away from the blackhole node W than it is from the screening node M. As a result, trust ratings of vertices in a single path to W via N remain unchanged, but when W is tested through node M, their confidence level will alter.

Algorithm-2

Let the kinds of attacks $t = 0$.

Select a first-time acceptable supervision approach $m^0(d)$.

Select the damage local network that is sufficient in size b.

With $m^t(d)$, compute the iterative value function $T^t(d)$ by

$$T^t(d(h)) = a(d(h/2), m^t(h/2)) + T^t(d(h/2+1)$$

Modify the incremental strategy $m^{t+1}(d)$ with $T^t(d)$ by

$$m^{t+1}(d(h/2)) = -(1/2)L^{-1}g^1(d(h/2))\overline{T}(d(h/2+1)$$

if $\|T^t - T^{t-1}\| \leq b$, halt to determine the best strategy $m^{t+1}(d)$;

If not, set $t = t + 1$ and return to the procedure.

In Algorithm 2, array A will be sorted according to the method with the lowest RTT among those created by the AOMDV, protocol. The path with a confidence greater than zero will then be found by checking all other routes. Array A is utilized to find the path wherein the amount of trust is zero in spite of anything.

According to [4], many protocols are used in data transfers between various systems. RTT deterioration is dependent on the connection type, such as whether it is a long- or short-term connection.

Similar to the literature [3–8], TPIDS used anomalous detection to determine whether or not the network had been accessed by the attacker. While the system has its foundation on the ARMA flow anomaly recognition framework, it employs a different approach. Whether flow estimations, examination, and identifying anomalies have been finished or not, each node communicates gathering data at the same time. TPIDS is a quick and easy way to find anomalies, and it has an excellent rate of identification for all kinds of assaults that can cause unusual alterations to traffic, according to simulation study, and it has low calculation overhead for nodes and minimum network communication expenses.

4. Results and Discussion

This research argues that the test strategy serves a crucial purpose for the WSN applications Scene. We presume that WSN is entirely secure during the deployment phase, that the security agreement in place for WSN [8] holds true, and that if we adopt the necessary security precautions and follow the deployment plan, it will be simple to implement. Since we assume that sensors on the links layer are functional, such as the the flow layer of protocol, a security reliance can be placed on the functioning of these commitments without being dependent on any particular arrangements.

The investigation and reaction phases of WSN systems that detect intrusions are standard. The first scenario describes the transfer of data acquiring finished on networks detect anomalies, and alarm details will be transmitted to the primary nodes or indicates collapse; The former defines why a node or networks go under, and the second can perform more advanced decision-making related to IDS and assault, for instance can adjust recognize the protocol for navigation, the node This study focused on how to identify abnormalities brought on by an invasion rather than choices or defenses.

TPIDS is a prominent target for numerous assaults, like radio frequency interference, particular E-attacks, floods attacks, sink incidents, and black hole assaults since it depends on flow estimation and prediction. For further attacks, including tunnel attacks, attacks with Sybil, altered and faked packets, etc. For details on complementary preventive actions not included in this paper, the audience is referred to [19].

4.1. Evaluation of alarming events and rates of detection

In this part, we compare TPIDS's various schemes based on the criterion for detecting efficiency in mathematical calculations. We evaluate finding accuracy using the indicators of the recognition rate and the false positive rate. They are noted in the vengeful packet corruption ratio's stated wording, which includes the reported amount of unauthorized lost packets, and the disclosed amount of quasi-detected and fraudulent activity packet losses.

4.2. Protocol Complexity

Implementing reactive conventional routing methods like AODV requires the use of three techniques: surveillance, firmware changes, and netfilter. Our EBR technique employs the AOMDV protocol, a multiple path variation of the AODV protocol. As a result, our suggested technique requires a similar amount of routing space as the implementation of AOMDV. Similar protocols include SUPERMAN [27] and others. However, as the number of nodes grows, SUPERMAN incurs significant overhead.

Algorithms 1 and 2 will be applied regularly performed to filter out the paths altered by AOMDV, preventing data from traveling through doubtful routes (going over a black hole nodes) or congested routes. If route to the target node aren't currently accessible on the sender end, a route creation procedure is launched when the AOMDV standard and the 3rd algorithm are active. At a result, many reliable routes are provided. The EBR route filtration will not affect the execution duration for the route choosing using AOMDV. However, since there will be fewer data retransmissions, using those dependable routes for data communication will obviously result in time savings. When weighed against then resorts methods, the modeling results showed increased network reliability, demonstrating this.

4.3. Design and Development

The overall goal of the research flow is to enhance and add to some of the existing research methods in order to give a better load balancing mechanism. To achieve effective routing and WSN attacks, new improvements to existing algorithms could be fine-tuned.

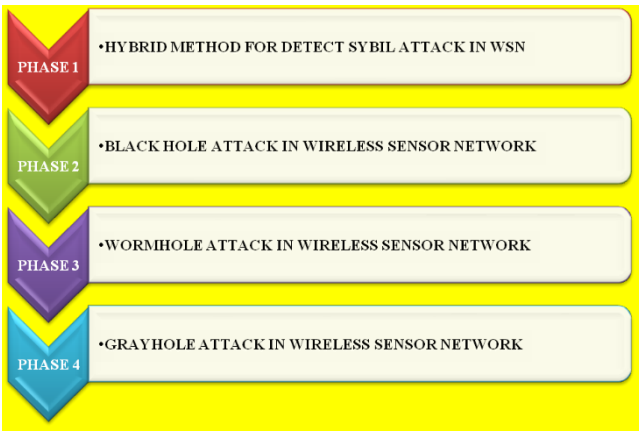

Fig. 1. Different phases to detect Black hole

Phase – I - HRP Protocol Based On ZH to Detect Black Hole Attack in Wireless Sensor Network

Here, we present the Hybrid Routing Protocol (HRP), which identifies the black hole attacker node and further prevents the attack from happening, as a solution for black hole attack detection and prevention. A hierarchical protocol built on the GPS (Global Positioning System) is called HRP (Hybrid Routing Protocol). It resembles Zone-based Hierarchical Link State in several ways. We build the routing zone in the suggested component out of sensor nodes. Nodes that can communicate with one another are found in the routing zone. The sensor nodes choose a zone head (ZH). Two factors must be taken into consideration while choosing a zone head.

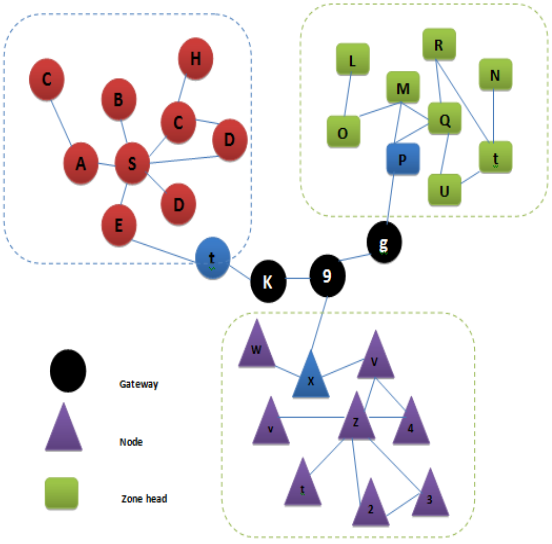

Fig. 2. Architecture Hybrid Routing Protocol

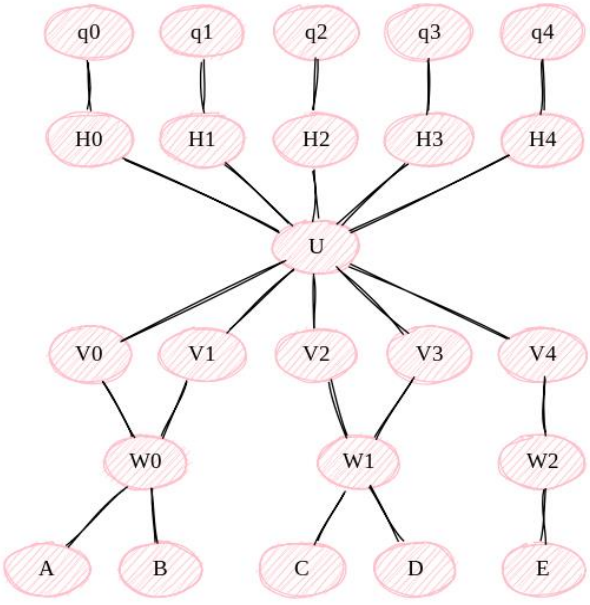

Fig. 3. Various paths along with nodes in blackhole

Each node uses a shifting method to pinpoint its exact setting, and by plotting its position on the region's map, it can also pinpoint its zone ID. Once every node has this zone ID, it can begin the within zone clustering followed by the interzone grouping structures to construct its routing tables.

Table1. Number of nodes with respect to their ID's

ID Assignment	
Node	ID
R1	IDR1
R2	IDR2
-	-
Rn	IDRn

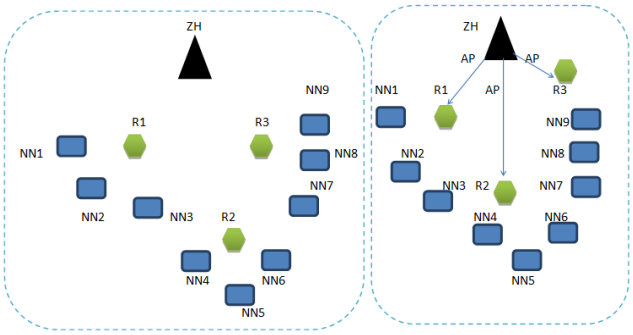

Fig. 4. Routing Zone head Formation and Id Assignment and Authentication Request

Table 2. Different routes with respect to the intermediate nodes in first cycle of Phase 1

Route	ID1	ID2	ID3	ID4
Route 1	8.2046	9.1532	8.207	7.2046
Route 2	8.163	9.1768	8.184	7.163
Route 3	10.239	9.2045	8.1827	7.239
Route 4	10.0949	9.0192	8.0434	7.0949
Route 5	10.2464	9.2264	8.1696	7.2464
Route 6	10.1832	9.2046	8.2318	7.1832

The procedure of an authentication request is shown in Figure 4, in which the zone head of the network sends an authentication packet (AP) to each and every sensor node as per table 1. The ID of the intermediate node is one of the two fields in this authentication message, and a piece is set to make it possible to identify it as an authentication packet (AP) as per table.

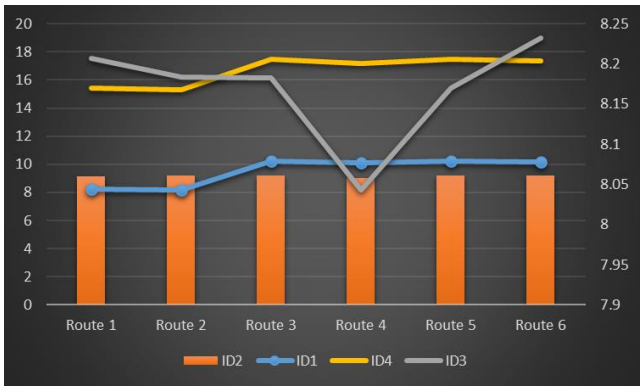

Fig. 5. Representation of Different routes with respect to the intermediate nodes infirst cycle of Phase 1

If not for some of the most common useful operators which are shown in figure 5, which are the blackhole nodes produced by an irrational spin of the circumference. Assume that $K^1 = F/V$ and $H(g) = g + k$ and k are dynamic nodes in a network. Let's take into account the proportional change operations of the kind in the region $\boldsymbol{P}_2(K^1)$

$$Mb(g) = p(g)b(g + k), g \in K^1 \qquad (1)$$

In actuality, earlier in other contexts, the blackhole nodes appearing in conjunction with the aggregating challenge for the users of the form (1) were taken into consideration. So, from the standpoint of the with an average challenge and an issue of lowering to the blackhole resistance form, we provide the established facts of the blackhole attacker in concept.

Let's first highlight a key distinction between differential equations and the blackhole nodes under investigation. Take the most straightforward inequality summing example. The series of inequality equations has the following form

$$\frac{\partial b_q}{\partial g} = p(qg)b_q(g) \qquad (2)$$

where $(g) = 1 + \frac{1}{2}\cos(2\pi g)$, then let's think about the packets for routing

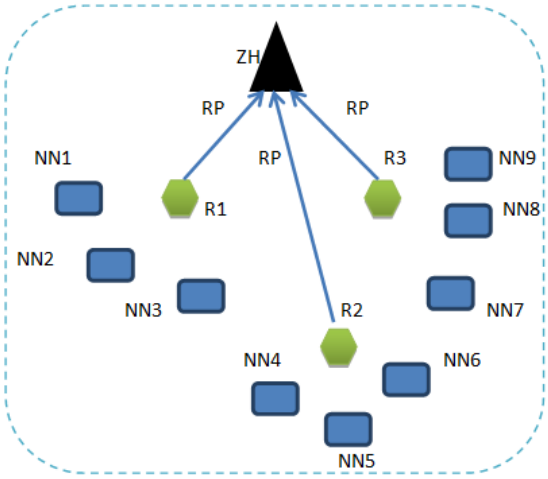

Fig. 6. Authentication Receive Process

Table-3. Different routes with respect to the intermediate nodes in second cycle of Phase 1

Route	ID1	ID2	ID3	ID4
Route 1	10.149	8.1545	9.1545	9.2339
Route 2	11.859	8.2276	9.2276	9.2141
Route 3	13.249	8.215	9.215	9.2647
Route 4	14.256	8.1051	9.1051	9.2264
Route 5	15.167	8.235	9.235	9.1986
Route 6	16.249	8.1571	9.1571	9.2478

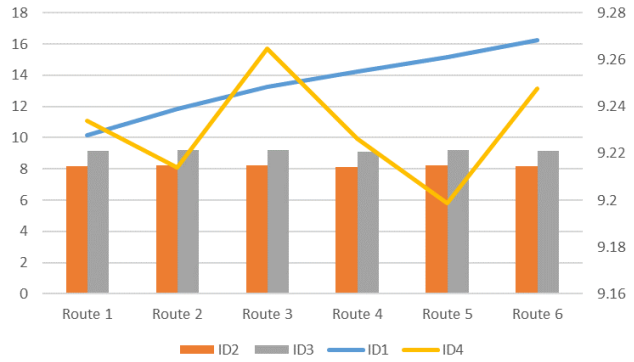

Fig. 7. Response Packet Fields

Figure 7 and table 3 shows the layout of the answer Packet (RP), which has two fields: the ID of the intermediary node and the ACK field with a specified piece set.

$$b_q(0) = b_0. \qquad (3)$$

The parameters $p(qg)$ of blackhole attackers and $p(g)$ simultaneously have an average worth of large q.

$$\overline{p} = \lim_{m \to +\infty} \frac{1}{m} \int_0^m p\,(g) \boldsymbol{B} g = 1. \qquad (4)$$

Thus, the calculation with pooled value has an inherent formulation

$$\frac{\partial b_0}{\partial g} = \overline{p} b_0(g)\,. \qquad (5)$$

According to comparing concepts, for the formula with the estimated factor, the outcomes of $b_q(g)$ tend to correlate with $b_0(g)$, the routing packets response. Let's now think about the order of weighting change processors. These fields are used for authentication to show that the answer is actually coming from the node.

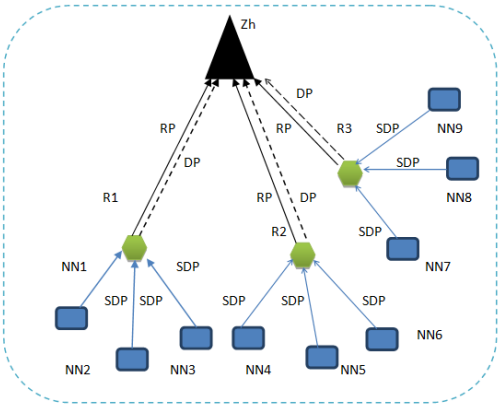

Fig. 8. Normal flow of traffic in WSN

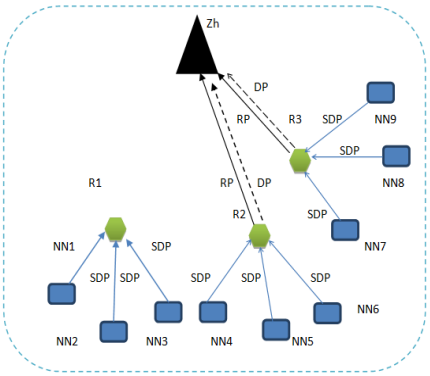

Fig. 9. Intermediate Node (R1) Failure

Figure 8 shows the typical flow of traffic in the WSN. Sensed Data Packets (SDPs) are sent to the router nodes by neighbor nodes (NN1, NN2,and NN9) after they have captured information on physical phenomena.

Table-4. Different routes with respect to the intermediate nodes in third cycle of Phase 1

Route	ID1	ID2	ID3	ID4
Route 1	7.5059	7.0911	7.9607	7.0956
Route 2	6.6066	7.0473	8.0713	7.074
Route 3	8.0075	7.0393	7.988	7.0595
Route 4	8.0085	6.9968	8.0803	7.0204

Route 5	6.5162	7.0698	8.0017	7.088
Route 6	8.3174	6.9795	8.0509	7.0065

Router nodes further process this data before sending it as a Data Packet (DP) to the cluster coordinator node as per table 4. Figure 9 shows that the router R1 does not respond to the zone head with a Response Packet (RP) and Data Packet (DP). Zone head waits for a predetermined amount of time (wtm). The node (R1) has failed if it fails to send any of these packets even after this amount of time has passed.

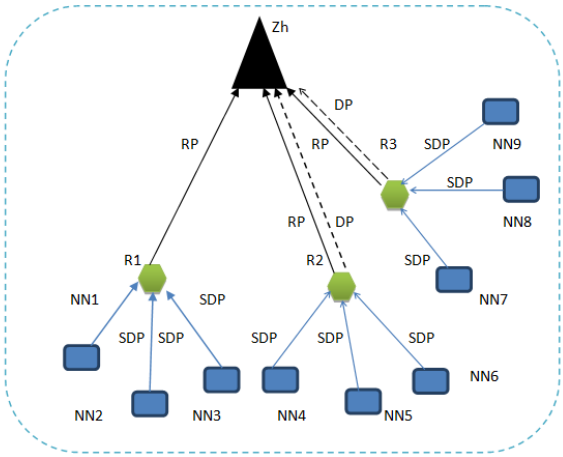

Fig. 10: Traffic Flow under Black hole attack

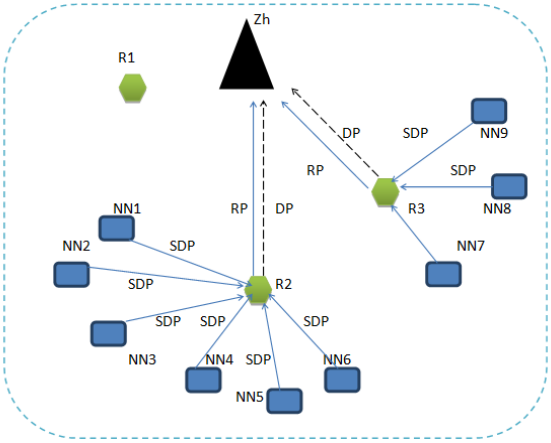

Fig. 11: Detection of Black hole attacker node

As it utilizes all the Sensed Data Packets (SDPs) coming from the neighboring nodes without sending them to the zone head, R1 Router in Figure 10 turns into the black hole node. The identification of router R1 as a black hole node by the coordinator is shown in Figure 11 as it is apparent from the fact that it is delivering response packets (RP) but not data packets (DP).

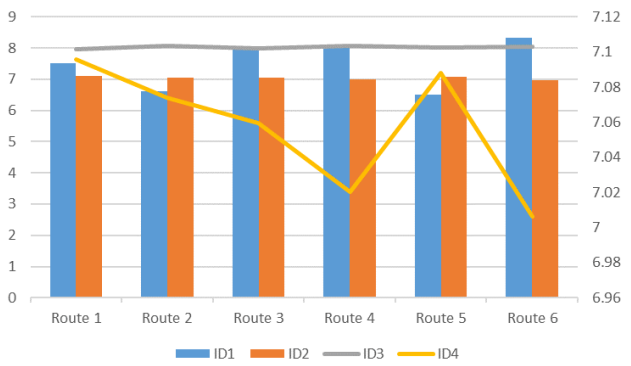

Fig. 12: Representation of Different routes with respect to the intermediate nodes in thirdcycle of Phase 1

Phase II - HRP Protocol Based On Zhls to Detect Black Hole Attack in Wireless Sensor Network

The Routing zone is changed by removing node R1 following the discovery of the black hole node (in this case, R1) in figure 12. Initially responding to router R1, neighbor nodes NN1, NN2, and NN3 are now providing SDPs to R2. In this way, the network achieves the usual evolution of traffic as given in figure 13,14,15 and 16.

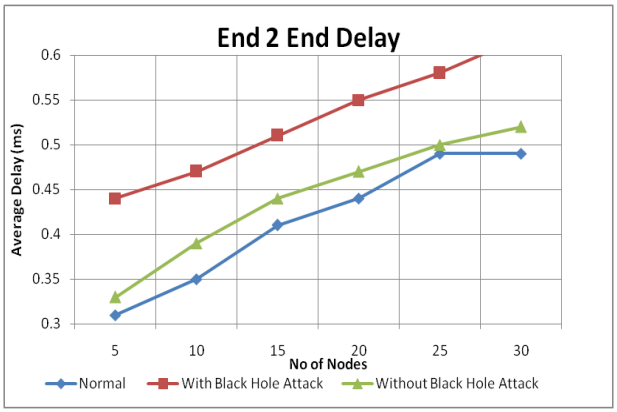

Fig. 13. End 2 End Delay in Hybrid Routing Protocol

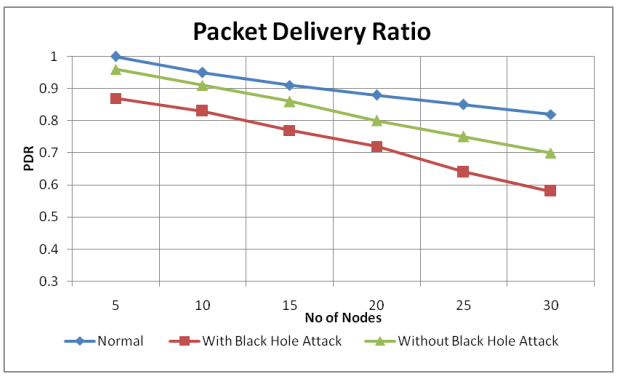

Fig. 14. Packet Delivery Ratio in Hybrid Routing Protocol

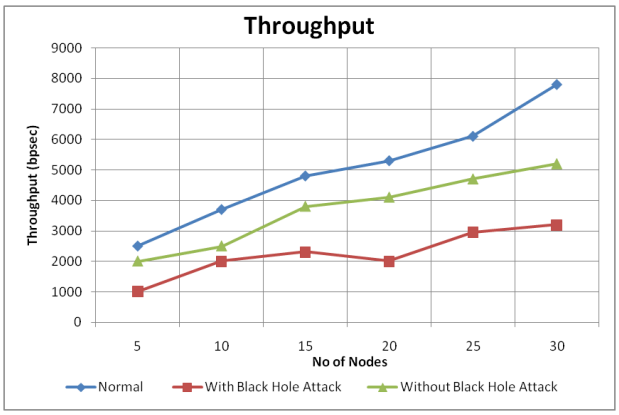

Fig. 15. Throughput in Hybrid Routing Protocol

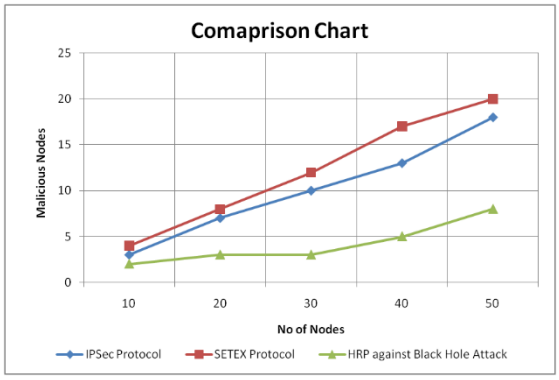

Fig. 16. Comparison Table of Black Hole Attack Detection

Table5. Different routes with respect to the intermediate nodes in first cycle of Phase I1

Route	ID1	ID2	ID3	ID4
Route 1	4.2358	4.771	4.8473	4.8795
Route 2	3.2145	4.9103	5.0305	4.9266
Route 3	2.6917	4.8526	4.9154	4.8845
Route 4	3.5828	4.8598	4.6743	4.9152
Route 5	3.4834	4.9493	4.9577	5.2313
Route 6	4.5835	4.8628	4.9401	4.9072

$$M_q b(g) = p_q(g) b(\alpha(g)) \qquad (6)$$

where the blackhole node values,

$p_q(g) = 1 + \frac{1}{2} \cos(2\pi q g)$, are precisely the same as in the equations (6). At first view, changing the ratio in the Indeed seems fairly natural as shown in table 5. The destination node of form (1) with infinite coefficient's harmonic width for irrational k is

$$w(M) = \exp\ k|p(g)|\boldsymbol{B}g \qquad (7)$$

$$\exp\left[\int_0^1 \ln\ |p_q(g)|\boldsymbol{B}g\right] \leq 1. \qquad (8)$$

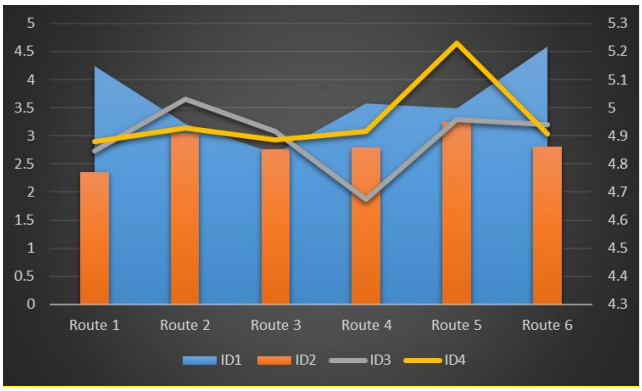

Fig. 17: Representation of Different routes with respect to the intermediate nodes in firstcycle of Phase I1

According to (7), the power of the component for the median of its exponent decreases to the target node for the blackhole attacker of the form (1) whose wavelength radius is preserved and given in figure 17.

In the event where the factor an is a routing protocol and the integer h is irrational, then for $|a(x)| > 0$ we have

$$J(M) = \{G : |G| = egp[\int_0^1 \ln\ |p(g)|\boldsymbol{B}g]\}, \qquad (9)$$

and in the case when ess inf $|p(g)| = 0$we have

$$J(M) = \{G : |G| \leq \exp\left[\int_0^1 k\,|p(g)|\boldsymbol{B}g\right]\}. \qquad (10)$$

Table-6. Different routes with respect to the intermediate nodes in second cycle of Phase I1

Route	ID1	ID2	ID3	ID4
Route 1	5.4911	6.5559	7.1105	6.8703
Route 2	8.2522	6.4837	6.8102	6.799
Route 3	6.6726	6.9606	6.3071	6.7835
Route 4	7.3929	6.8011	6.7524	6.8092
Route 5	5.2751	6.7381	6.8123	6.7494
Route 6	6.2411	6.8035	6.8273	6.8105

The above description was found in [3] regarding constant coefficients, and the proof applies to routing protocol functions as well. The comparable requirement is the requirement that a function K specifies an association that includes two balanced shift operators. The equality is represented as $Kp_1T_kK^{-1} = p_2T_k$.

$$p_1(g)\frac{f(g)}{f(g+k)} = p_2(g) \qquad (11)$$

If an expression f exists that satisfies the condition of equality (2.6), then the functions p_1 and p_2 are considered destination nodes and are equal. In particular, the modulo

operator pT_k is analogous to an operator with an invariant coefficient if its value p is the destination node equivalent to a constant.

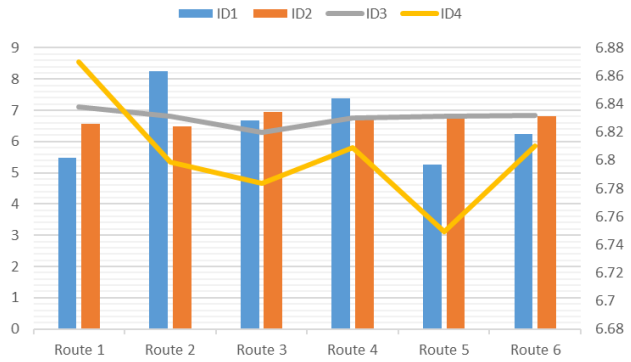

Fig. 18: Representation of Different routes with respect to the intermediate nodes insecond cycle of Phase I1

The destination node similarity of a progressive polynomial p to a constant ζ is now the subject of a distinct formulation that will be discussed.

$$p(g) = \zeta \frac{f(g)}{f(g+k)}. \quad (12)$$

A factorization using a modification is an illustration of the coefficient p in the form (12).

For$p(g)$ and $\boldsymbol{B}(g) = \ln f(g)$, the known destination node calculation is implied by linear equivalency (12).

$$\boldsymbol{B}(g) - \boldsymbol{B}(g+k) = \boldsymbol{E}(g) - \ln \zeta, \quad (13)$$

if the unknowns are steady and function $\boldsymbol{B}$. We note that the function $\boldsymbol{B}$ must be restricted in order for the operator K to be invertible. Numerous situations involve equation (2.8), which is thoroughly explored. The domain of $\zeta_0(K^1)$ composed up of functions that are matching the requirement will be denoted by the symbol $\zeta(K^1)$.

$$\int \boldsymbol{E}(g)\boldsymbol{B}g = 0. \quad (14)$$

The requirement $\boldsymbol{E} - \ln \zeta \in \zeta_0(K^1)$ setting the number ζ in a special way is a need for issue (14) to be solvable.

Discussions

The black hole is one of the attacks on MANETs. It only happens when a malicious node deceives other nodes into believing it has the shortest path between source and destination before destroying all packets it receives. Figure 1 depicts a sample of this kind of assault. Node A, the input node, and then needs to convey information to node I, the node that is the destination, as seen in Figure 1. A, B, G, and I are plausible transmission pathways for this data, but node D in this case behaves destructively and asserts that it is the shortest route between source and destination. In response to A's route request (RREQ), it provides the wrong response. Therefore, the malicious node completely destroys every data packet it receives. Other types of black hole attacks combine various elements, and a small number of destructive nodes work together to cause damage that spreads throughout the entire network.

Routing disruption is one way to stop black hole attacks. It is advised to choose more than one path from source to destination while using this strategy. In each case, it is advised that at least three paths be chosen from source to destination. The packet containing the RREQ message is initially sent by the source node to the intermediate and destination nodes. Nodes that are able to build a route from the source to the destination respond to the source's request by sending it a route replay (RREP) message. The source stores the RREP packet it receives in its buffer in order to obtain two more pathways. All of the packets are then loaded into the buffer, where they are analyzed before the best route is chosen. Based on the number of nodes, the source node chooses the safest path and avoids the black hole assault. [9].

5. Conclusions

The study presented a novel idea that can identify and stop malicious intrusions while also choosing less crowded paths. This is done by using a protocol that appears to function properly in order to entice a malicious node to exhibit suspicious behavior. We described an Extra Blackhole Resistance (EBR) protocol in our appearance, which may be implemented into any proactive routing strategy in MANETs. Each node might use a combination of the time to live (TTL) and the round-trip time (RTT) to evaluate the level of certainty of nearby nodes, which could then be used for assessing the location of the a black hole network(s). EBR would choose the way with the shortest RTT, which suggests the least crowded paths, among the safe accessible routes. Our newly developed approach saves gas and computational capacity because it does not rely on encryption techniques. Furthermore, since EBR does not require any unique packets, the routing overhead is minimal.

We introduce a unique Stochastic template-based aberration detect the presence-based security approach for large-scale networks of sensors in this research. These statistics can be used subsequently to identify changes in them if each node is able to construct a straightforward Markov model of traffic prediction. We have demonstrated that a node is capable of identifying an intrusion pretending to be a trustworthy neighbor by examining a relatively small amount of incoming packet attributes.

We took into account the problem detection procedure used at each node individually in the way we did things. Collaboration algorithms with low complexity may enhance the process of detection and containment. Various medium-

access, distributed supervision, and routing strategies will introduce multiple characteristics. More investigation is required to identify improved node features that address particular vulnerabilities and to create improved detection procedures that take into account the capabilities of sensor nodes. When compared to AODV, AOMDV, and SUPERMAN, the EBR protocol clearly improves network performance, according to simulation results. The suggested technique finds blackhole locations quickly, despite the total quantity of antagonistic nodes along a path or the time at which they join a network.

References

[1] Acquisti, A.; Carrara, E.; Stutzman, F.; Callas, J.; Schimmer, K.; Nadjm, M.; Gorge, M.; Ellison, N.; King, P.; Gross, R. Security Issues and Recommendations for Online Social Networks; ENISA Position Paper No.1; ENISA—European Network and InformationSecurityAgency:Heraklion,Greece,2007;

Volume43.

[2] Huang,K.;Zhou,C.;Tian,Y.- C.;Tu,W.;Peng,Y. Application of Bayesiannet work to data-driven cyber- security risk assessment in SCADA networks. InProceedingsofthe201727thInternationalTelecommunicationNetworksandApplicationsConference(ITNAC),Melbourne,VIC,Australia,22–24November2017;IEEE:NewYork,NY,USA,2017.

[3] Kannan, R.; Ray, L.; Durresi, A.; Iyengar, S. Security-performance tradeoffs of inheritance based key predistribution for wireless sensor networks. *arXiv*2004.

[4] Elsaeidy,A.;Elgendi,I.;Munasinghe,K.S.;Sharma,D.;Jamalipour,A.Asmartcitycybersecurityplatformfornarrowband networks .In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, VIC, Australia, 22–24 November 2017; IEEE: New York, NY, USA, 2017.

[5] Reddy,G .A Delay Sensitive Multi-PathSelectiontoPreventtheRushingAttackinVANET.InProceedingsofthe20215th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 22–23 October 2021; IEEE: New York, NY, USA, 2021.

[6] Sayan,C.;Hariri,S.;Ball,G.Cybersecurityassistant:Designoverview.InProceedingsofthe2017IEEE2ndInterna-tionalWorkshopsonFoundationsandApplicationsofSelf*Systems(FAS*W),Tucson,AZ,USA,18–22September2017; IEEE: New York, NY, USA, 2017.

[7] Nair,R.;Ragab,M.;Mujallid,O.A.;Mohammad,K.A.; Mansour,R.F.;Viju,G.K.Impactofwirelesssensordata miningwith hybrid deep learning for human activity recognition.*Wirel.Commun.Mob.Comput.*2022, *2022*, 9457536.

[8] Tagarev,T.DigilienceAPlatformforDigitalTransformation,CyberSecurityandResilience.*Inf.Secur.*2019,*43*, 7–10.

[9] Hamdi,M.M.;Audah,L.;Abood,M.S.;Rashid,S.A.;Mustafa,A.S.;Mahdi,H.;Al-Hiti,A.S.Areviewonvarioussecurityattacksinvehicularadhocnetworks. *Bull.* Electr. *Eng.* Inform. 2021,10,2627–2635.

[10] Moustafa, A.A.; Bello, A.; Maurushat, A. The role of user behaviour in improving cyber security management.*Front.Psychol.* 2021, 1969.

[11] Stacey, T.R.; Helsley, R.E.; Baston, J.V. Identifying information security threats. *Inf. Syst. Secur.* 1996, *5*, 50–59.

[12] Sohraby, K., Minoli, D., and Znati, T.; "Wireless sensor networks: technology, protocols, and applications." *John Wiley and Sons*, 2007.

[13] Rawat, P., Singh, K. D., Chaouchi, H., and Bonnin, J. M. "Wireless sensor networks: a survey on recent developments and potential synergies." *The Journal of supercomputing*, 2014, 68(1): 1–48.

[14] Kalkha, H., Satori, H., and Satori, K.; "Performance Evaluation of AODV and LEACH Routing Protocol." *Advances in Information Technology*: *Theory and Application*, 2016.

[15] Nieles, M.; Dempsey, K.; Pillitteri, V. *NIST Special Publication 800-12 Revision 1: An Introduction to Information Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017.

[16] Zafar, F.; Khattak, H.A.; Aloqaily, M.; Hussain, R. Carpooling in Connected and Autonomous Vehicles: Current Solutions and Future Directions. *ACM Comput. Surv. (CSUR)* 2021, *54*, 218.

[17] Safaa,O.;Firas,S. On the Designing of two grains levels network intrusion detection system.*Karbala Int.J. Mod.Sci.*2015,*1*, 15–25.

[18] Rajasekharaiah, K.; Dule, C. S.; Sudarshan, E. Cyber Security Challenges and its Emerging Trends on Latest Technologies. In Proceedings of the International Conference on Recent Advancements in Engineering and Management (ICRAEM-2020), Warangal, India, 9–10 October 2020.

[19] Papamartzivanos,D.;Mármol,F.G.;Kambourakis,G.Dendron:Genetictreesdrivenruleinductionfornetworkin

trusion detection systems.*Future Gener.Comput.Syst.*2018, *79*, 558–574.

[20] Kabir, E.; Hu, J.; Wang, H.; Zhuo, G. A novel statistical technique for intrusion detection systems.*Future Gener.Comput.Syst.* 2018, *79*, 303–318.

[21] Salih, A.A.; Adnan Mohsin, A. Evaluation of classification algorithms for intrusion detection system:A review.J. Soft Comput. Data Min.2021, 2, 31–40.

[22] Palma,A.;Pereira,P.R.;Pereira,P.R.;Casaca,A.Multicastroutingprotocolfor VehicularDelay-TolerantNetworks. InProceedingsofthe2012IEEE8thInternationalConferenceonWirelessandMobileComputing,NetworkingandCommunications(WiMob),Barcelona,Spain,8–10October2012;pp. 753–760.

[23] Hemanand, D., Reddy, G. ., Babu, S. S. ., Balmuri, K. R. ., Chitra, T., & Gopalakrishnan, S. (2022). An Intelligent Intrusion Detection and Classification System using CSGO-LSVM Model for Wireless Sensor Networks (WSNs). International Journal of Intelligent Systems and Applications in Engineering, 10(3), 285–293. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2167

[24] P. Satyanarayana, U. D. Yalavarthi, Y. S. S. Sriramam, M. Arun, V. G. Krishnan and S. Gopalakrishnan, "Implementation of Enhanced Energy Aware Clustering Based Routing (EEACBR)Algorithm to Improve Network Lifetime in WSN's," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-6, doi: 10.1109/ICMNWC56175.2022.10031991.

[25] Gopalakrishnan Subburayalu, Hemanand Duraivelu, Arun Prasath Raveendran, Rajesh Arunachalam, Deepika Kongara & Chitra Thangavel (2023) Cluster Based Malicious Node Detection System for Mobile Ad-Hoc Network Using ANFIS Classifier, Journal of Applied Security Research, 18:3, 402-420, DOI: 10.1080/19361610.2021.2002118

[26] Satyanarayana, P., Diwakar, G., Subbayamma, B. V., Phani Sai Kumar, N. V., Arun, M., & Gopalakrishnan, S. (2023). Comparative analysis of new meta-heuristic-variants for privacy preservation in wireless mobile adhoc networks for IoT applications. Computer Communications, 198, 262–281. https://doi.org/10.1016/j.comcom.2022.12.006

[27] Perumal, G., Subburayalu, G., Abbas, Q., Naqi, S. M., & Qureshi, I. (2023). VBQ-Net: A Novel Vectorization-Based Boost Quantized Network Model for Maximizing the Security Level of IoT System to Prevent Intrusions. Systems, 11(8), 436. MDPI AG. Retrieved from http://dx.doi.org/10.3390/systems11080436

[28] Turaka, R., Chand, S. R., Anitha, R., Prasath, R. A., Ramani, S., Kumar, H., Gopalakrishnan, S., &Farhaoui, Y. (2023). A novel approach for design energy efficient inexact reverse carry select adders for IoT applications. Results in Engineering, 18, 101127. https://doi.org/10.1016/j.rineng.2023.101127