Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 9845793, 1 page
https://doi.org/10.1155/2023/9845793

Retraction

Retracted: Self-Adaptive Framework for Rectification and Detection of Black Hole and Wormhole Attacks in 6LoWPAN

Wireless Communications and Mobile Computing

Received 12 December 2023; Accepted 12 December 2023; Published 13 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] T. Kamaleshwar, R. Lakshminarayanan, Y. Teekaraman, R. Kuppusamy, and A. Radhakrishnan, "Self-Adaptive Framework for Rectification and Detection of Black Hole and Wormhole Attacks in 6LoWPAN," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5143124, 8 pages, 2021.

Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5143124, 8 pages
https://doi.org/10.1155/2021/5143124

Research Article

Self-Adaptive Framework for Rectification and Detection of Black Hole and Wormhole Attacks in 6LoWPAN

T. Kamaleshwar,[1] R. Lakshminarayanan,[2] Yuvaraja Teekaraman,[3] Ramya Kuppusamy,[4] and Arun Radhakrishnan[5]

[1]*Department of Computer Science Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, 600 062, Chennai, India*
[2]*Department of Networking and Communications, SRM Institute of Science and Technology, Kattankulathur, 603 203, Chennai, India*
[3]*Mobility, Logistics and Automotive Technology Research Centre, Faculty of Engineering, Vrije Universiteit Brussel, Brussel 1050, Belgium*
[4]*Department of Electrical and Electronics Engineering, Sri Sairam College of Engineering, 562 106, Bangalore City, India*
[5]*Faculty of Electrical & Computer Engineering, Jimma Institute of Technology, Jimma University, Ethiopia*

Correspondence should be addressed to Yuvaraja Teekaraman; yuvarajastr@ieee.org
and Arun Radhakrishnan; arun.radhakriahnan@ju.edu.et

Received 18 October 2021; Accepted 7 December 2021; Published 26 December 2021

Academic Editor: Rashid A Saeed

Internet network communication protocol version 6 low-power wireless personal area networks (6LoWPAN) is supposed to assist the gadgets with low-power wireless sensor network (WSN) and it furnishes the top model layer of the data transmission system. The 6LoWPAN is prone to the diversified attacks such as wormhole and black hole attacks, which might be very difficult to become aware of and defend. In a wormhole attack, the attacker listens to the facts over the networks, and in a black hole attack, the intruder reprograms the nodes to dam the data transmission. As an end result, any data datagram that enters the attacked region will end result in transmission failure with low flow network rate and excessive one-way delay. To come across and heal the attack, a self-adaptive framework is brought into the networks and the procedure of data transmission is enriched. In this work, the affected region is measured and rectified with the aid of using the proposed self-adaptive framework for Ad Hoc On-Demand Distance Vector (AODV) routing protocol network communication protocol. The overall performance of the network healing technique is investigated with the aid of using simulation and its miles diagnosed that the proposed framework suggests promising overall performance with the aid of using accomplishing excessive flow network rate and minimum delay.

1. Introduction

In WSN, the technique of network communication is mounted with the aid of using mote nodes, and the transmission is attained with the aid of using a wireless transceiver that has no self-governance or network infrastructure. The mote nodes are instilled with confined electricity and now have a network unreliable transmission medium [1]. WSN has various constraints and it outcomes in new challenges. IEEE 802.15.4 shows the wireless hyperlink and it is far embedded in diverse packages which are with the low-power network communication medium. 6LoWPAN is broadly utilized in a great deal tracking utility and it modifies the network communication protocol stack with the aid of using introducing an adaptation version layer in among the network version layer and IP stack hyperlink. The alteration in network communication protocol permits powerful IPv6 datagram transmission and additionally minimizes the IP overhead [2]. 6LoWPAN has met with diverse problems during data transmissions consisting of the confined length of the datagram, routing

protocol, IP connectivity, topologies, confined network configuration, and protection discover [3]. 6LoWPAN is categorised into hierarchical routing protocol, location-based routing protocol, and multihop routing protocol. The multihop routing protocol and network communication protocol AODV is particularly focused that is a sufficiently robust routing protocol technique and it is far suitable for 6LoWPAN that is network dependable in figuring out the optimal path [4]. AODV permits terminal node to gain the new paths and discards the inactive links. When a neighboring node faces any hyperlink breakage because of a protection data breach, the nodes in the transmission networks must provoke the path discovery technique with the aid of using propagating a brand new RREQ. In a black hole attack, the attacker captures the transmission node and reprograms the node to dam the transmission [5]. The routing protocol framework is destabilized with the aid of using the era of faux street era that ends in studying the records transmitted over the networks. The failure or network miscommunication is completed with the aid of using various protection attacks, and hence, 6LoWPAN proposed a self-adaptive framework with the nearby repair. On the safety level, 6LoWPAN faces various protection attacks and reason protection breakage in the networks. Overall data transmission with a 6LoWPAN is displayed in Figure 1.

Wormhole attacks create a sufficiently robust tunnel and a number of the distant routers and alter the routing protocol conduct and transmit the visitors via the tunnel [6]. This state of affairs makes the sufferers pick out the shortest path, and the long way apart routers observed close to the neighbor. Wormhole attack is carried out to a head important records with high waft rate. The wormhole is not always an important protection data breach; however, it mixed with any other attack which is a sink hole that could be an important protection threat. Black hole attack is a denial-of-service (DoS) attack and it disturbs the overall performance of the data transmission. The attacks may be generated through high-power wireless hyperlinks, and 6LoWPAN is notably susceptible to sink hole attack [7, 8]. Excessive one-way delay is the length of the time that a packet takes from point A to point B across the network and one-way delay measurement based on low flow data in large enterprise networks.

The records entered via the attacked mote node do not attain the end point and this consequences in decreased waft rate and postpones withinside the transport of the datagram [9]. So, the method of identity and rectification of attack withinside the networks is important for effective data transmission over the networks. In this work, a self-adaptive framework is proposed and the nearby restore method is initiated that enriches the data transmission. In this framework, a coordinating mote node is chosen primarily based totally on performance and fairness. The mote node withinside the coordinating role is answerable for the verification of neighboring node failure, authorization, and the detection of attack is gift with inside the transmission networks [10].

The research article is organized as follows: Section 2 elaborates the latest evaluations and disadvantages withinside the research, Section 3 explains the proposed prevention and recovery framework, Section 4 illustrates the simulation evaluation, and Section 5 offers the destiny scope and conclusion.

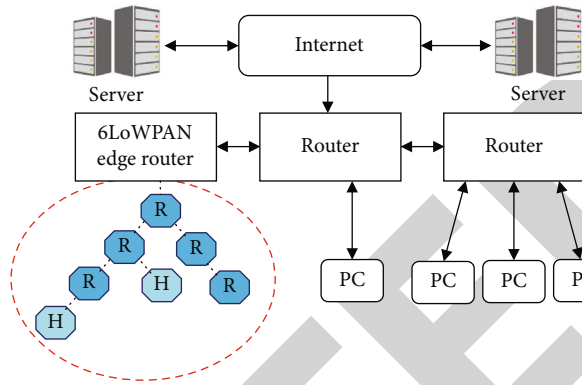
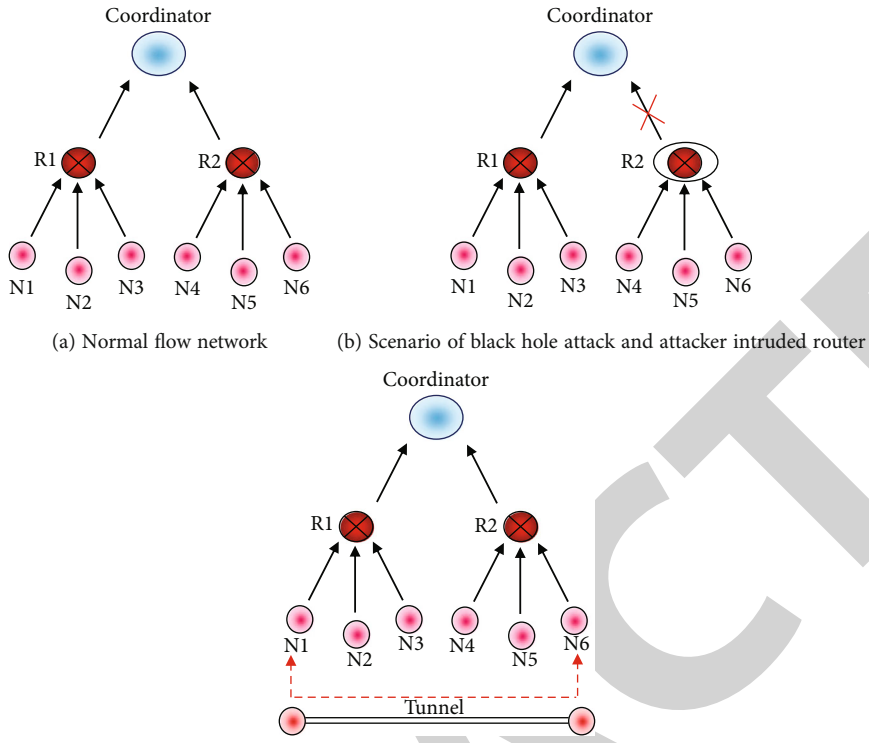


Figure 1: Schematic representation of the IPv6 transmission networks with a 6LoWPAN.

2. Related Work

2.1. 6LoWPAN and RPL. The 6LoWPAN became utilized in a small get admission to point with the limited power delivery that determines the workings of header compression and hidden data from the user. It makes use of the Internet network communication protocol (IP) to alternate and talk the data over the networks. RPL low power and lossy network (LLN) is a data transmission network communication protocol that became integrated in minimal electricity utilization get admission to point and in charge to datagram loss. The network communication protocols IPv4 and IPv6 have been the predecessors of 6LoWPAN that inherit the safety troubles from diverse factors, and IP spoofing became a typical attack. 6LoWPAN became an unsecured wireless medium that necessitates diverse safety factors to safeguard data transmission [11] and it became extensively implemented to get admission to point with minimum latency. The mobility control structure became proposed in [12] for effective routing protocol to acquire mobility and network topology control. This framework makes use of methods particularly tough and tender handoff in which identity of the latest links is earlier than hyperlink breaks and disconnection of hyperlink, respectively. The mRPL+ carries the 6LoWPAN/RPL stack in a well suited way and additionally carried out higher results [12].

2.2. Attacks in 6LoWPAN. The Sybil and wormhole attack become recognized with the proposed LiDL framework and it evolved the Highest Rank Common Ancestor (HRCA). The nodes withinside the networks have been organized to assemble a tree and from the tree maximum rank or ancestor become detected with the aid of using HRCA. The intruder node withinside the networks is recognized, and the system of mitigation of lightweight node becomes initiated. The attack becomes rectified and attained the satisfactory end result with the aid of using the proposed framework [13]. An intrusion detection system becomes designed to come across the wormhole attack, and the



(a) Normal flow network

(b) Scenario of black hole attack and attacker intruded router

(c) Scenario of wormhole attack and attacker creates tunnel to listen the information

Figure 2: The overall attack scenario.

```
1. start
2. if event==Network_In_Event then
3. if packet==control_packet then
4. check if node==MaliciousNode then
5. set the rank of the present node=Malicious Rank
6. else
7. process the message
8. endif
9. else
10. endif
11. if node==packet and malware node is notempty then
12. drop the message
13. endif
```

Algorithm 1: Pseudocode for implementation of sink hole with black hole attack.

detection rate is improved [14]. The safety functionality becomes investigated, and novel measurers have mentioned in [15] that safety components play an essential position in 6LoWPAN/RPL.

6LoWPAN is extraordinarily prone to vulnerabilities, and plenty of styles of attacks have been explored. Varied styles of safety answers have been explored, and the drawbacks of the answer for the 6LoWPAN attack are examined. The research hole withinside the current set of rules becomes reviewed, and rectification measures have been mentioned [16]. An Ant Colony Optimization Boolean Expression Evolver Sign Generation (ABXES) set of rules becomes projected to identify the anomalous hyperlink and perceive the attack. The identity workings in ABXES become a critical problem and the putoff is high [17]. The identity of intrusion in RPL primarily based totally on 6LoWPAN becomes evolved, and the visitors' sample of the projected set of rules becomes tough to identify and rectify. The glide rate of the set of rules becomes relatively near the current framework [18, 19]. The black hole attack rectified the usage of the cryptography workings and putoff is high [20]. The research hole recognized with inside the literature part is rectified with the aid of using the proposed framework and mentioned in Section 4.

1. A malicious node is taken, which is defined as a macro with its ID as well as rank.
2. Hash function is used to randomly generate the rank for the malicious node.
3. In NETWORK_IN_EVENT, the random rank generated is assigned to the malicious node.
4. If randomly generated rank is 1, then the value is incremented.
5. If data packets are coming on malicious node, then those packets are dropped, thus decreasing the flow network rate of the system.
6. If the randomly generated value is divisible by 2, then packet was not allowed to be forwarded.
7. Otherwise, it was forwarded normally.
8. Whenever a NETWORK_IN_EVENT takes place at malicious node, it keeps on forwarding DIO messages for a finite number of time.
9. In that time will be added to the neighbor list of other nodes.
10. A node is made malicious node and whenever a network-in event takes place at this node, the ID of this malicious node is cloned with an another node.
11. This attack creates confusions in the network. This attack results in the changing of rank of both malicious node and with whom the malicious node is being cloned.

Algorithm 2: Incorporation of attack and hash function assignment.

1. start
2. if event==NETWORK_IN_EVENT2.then
3. if packets==control packets and are DIOmessages then
4. if previous node is notnull then
5. ID and rank of previous node are restroed to its previousvalues
6. The rank and ID of current are stored in prev_node_id and prev_node_rank respectively.
7. The rank of current node is changed toINFINITY.
8. Endif
9. endif
10. if packets==data packets and currect node has rank==INFINITY then
11. drop themessage
12. endif
13. endif

Algorithm 3: Pseudocode of local repair attack.

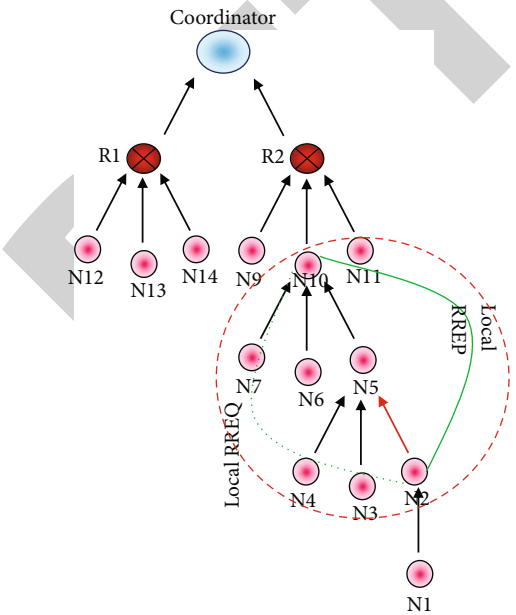


Figure 3: Data transmission via attacked region.

2.3. Detection of Black Hole and Wormhole Attack. Black hole attack denies the transmission method and it is far a type of DoS attack wherein the router (R2) is meant to transmit the datagram rather it drops the datagram. The breakage of the hyperlink and the data transmission interruption is proven in Figure 2(b). In the black hole attack, the attacker captures the functionality of the node and reprograms the node that blocks the data transmission. The data entered into the black hole region is captured and reprogrammed. Black hole attack is straightforward to find out and additionally undermine through the network partition approach. The prevalence of a black hole in the transmission location reduces the float rate and will increase the delay.

Wormhole attack is a type of routing protocol attack and it is far initiated on the network version layer that is usually on the remote role which however pretends as a neighbor. The wormhole friends set up the tunnel or hyperlink throughout the nodes in the networks, and the routing protocol network communication protocol corrupted the use of the installed tunnel. Wormhole attack is carried out to transmit the private statistics throughout the channel with high float rate and it is not a severe safety issue. The attacker initiates an aggregate of any attack with a wormhole attack that is taken into consideration as sink hole attack and it reasons

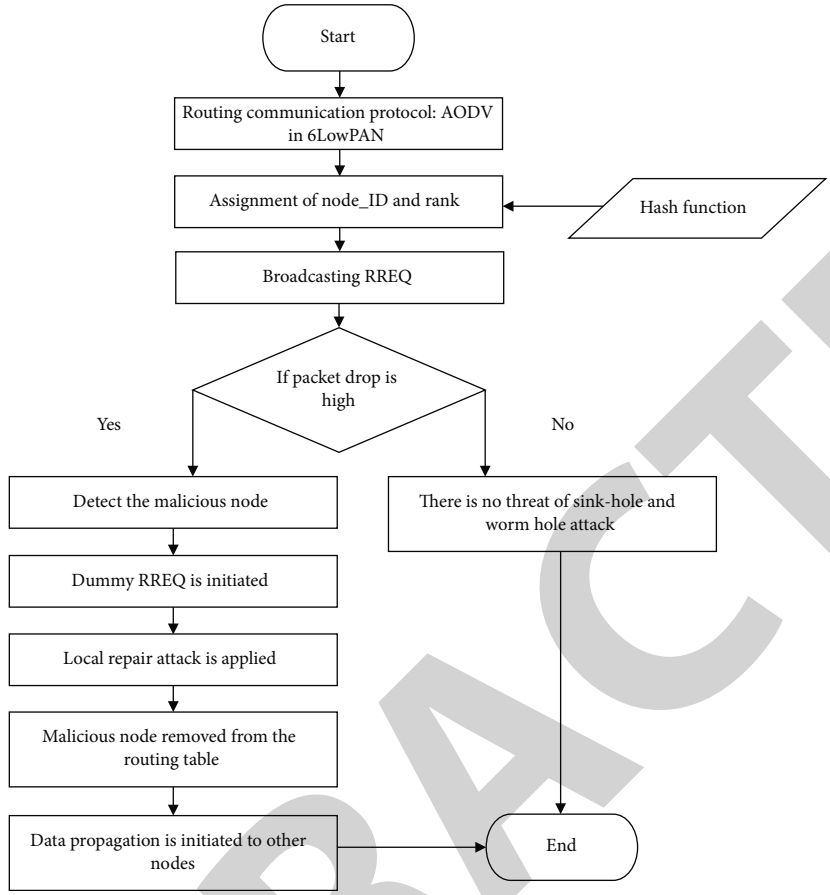


Figure 4: Overall transmission framework and local repair technique.

Table 1: Compression of flow network rate.

No. of nodes	AODV	Native AODV with BH	Modified AODV
25	40	70	110
50	30	130	170
100	45	90	140
150	42	110	172

Table 2: Compression of flow network rate.

No. of nodes	XMAC	TBBT	AODV with BH
25	90.05	82.388	39.162
50	141.65	137.527	26.644
100	86.541	90.642	40.051
150	123.02	121.6	37.148

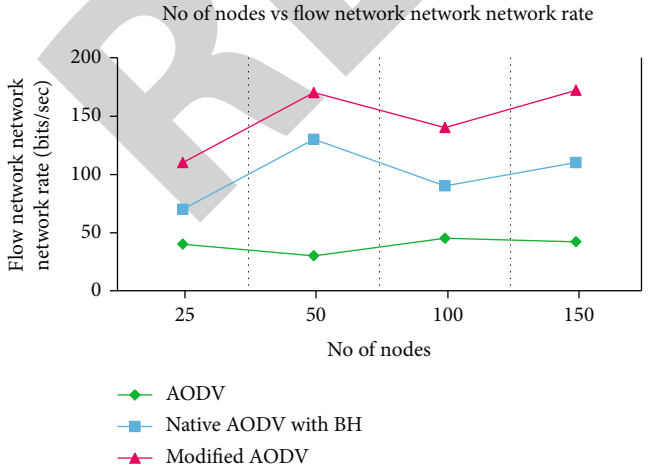


Figure 5: Compression of flow network rate.

severe safety data breach in the transmission environment. The attacker creates a tunnel of the use of various procedures, namely, network communication protocol distortion, datagram relay, datagram encapsulation, and high-quality transmission. The tunnel introduction and the intrusion are illustrated in Figure 2(c).

In Figure 2(a), the normal flow network of the data datagram is shown. In this context, 2 routers (R1 and R2), 6 mote nodes (N1, N2, N3, N4, N5, and N6), and a coordinator were presented. The mote node feels the environmental phenomenon, and the sensed records are transmitted to the respective router. The router transmits the data to the coordinator for the in addition decision-making method. Figure 2(b) shows the black hole attacking situation. The router R2 is attacked, and the transmission is interrupted on the router region. Figure 2(c) shows the wormhole attacking situation. A sufficiently robust tunnel is created

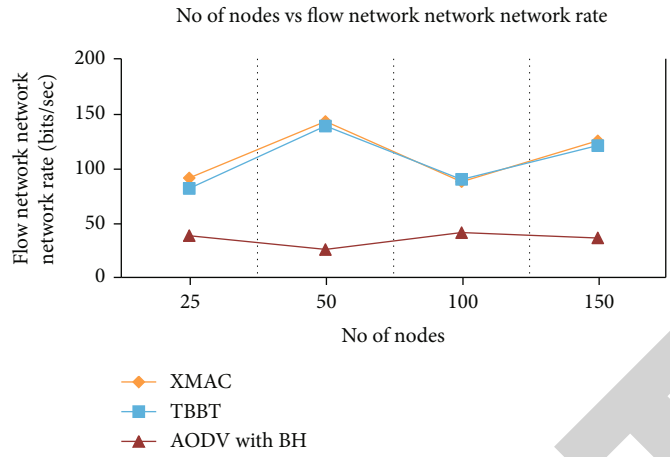


Figure 6: Compression of flow network rate.

Table 3: Compression of one-way delay.

No. of nodes	AODV	Native AODV with BH	Modified AODV
25	1.12	1.32	1.19
50	0.8	1.12	1.15
100	0.79	1.05	0.93
150	0.68	1.35	0.83

in the mote node region, and the attacker listens to the records transmitted throughout the tunnel.

In the AODV network communication protocol, the attack is initiated in the path discovery section. Wormhole friends generate the phantasm of neighbor at one hop, and the path request (RREQ) datagrams are transmitted through the tunnels to attain the node on the end point that discards the complete RREQ datagram. The hit inclusion of wormhole friends and tunnel in the transmission path makes selective forwarding, delays the datagram transmission, and introduces false routing protocol. Thus, wormhole distorts the transmission of data and listens to the personal records.

The wormhole and black hole attacks bind collectively and its miles initiated into the AODV network communication protocol on the RREQ section that breaks the transmission link. The data transmission is intruded, and the networking situation is reprogrammed to discard the routing protocol method. The identity of intrusion and rectification of the attack is mentioned in the subsequent part. The rectification of attack will increase the data transmission method and obtain excessive overall performance withinside the transmission.

3. A Self-Adaptive Framework for the Prevention of Black Hole and Wormhole Attack

In this part, the proposed working with neighborhood restore in AODV is discussed. Initially, mote nodes are deployed in the transmission surroundings and the attack is applied in the transmission link. The ID era is carried out with the aid of using the hash function, the transmission with intrusion rectified the usage of neighborhood restore, and the data is transmitted alongside the rectified region. The hash function desk is often up to date and the rank for the node is randomly up to date. The shortest path and effectiveness are carried out the usage of the proposed self-adaptive framework.

3.1. Sink Hole with Black Hole Attack Incorporation in 6LoWPAN. The mote nodes are deployed in the transmission networks, and each node is assigned with a completely unique ID. Before the project of the ID to the node, the attack is carried out to the networks. Initially, sink hole and black hole attack is included into the networks that discard the transmission with the aid of using breaking the link. The attacked node in the networks is diagnosed as an intruder node, and each node in the networks is assigned with node_ID which is the rank. The rank technology performed the use of the hash function on the NETWORKS_IN_EVENT, and the rank acts as a gateway of the system. During the NETWORKS_IN_EVENT, DIO messages exchanged for a finite quantity of instances to attain the end point and the routing protocol statistics in addition to the neighbor node listing statistics which is up to date into the routing protocol table. The incorporation of attack and hash function initialization is given in Algorithm 1.

14. stop

3.2. Identification of Intruder Node and Intruded Region in the Networks. In this proposed self-adaptive framework, the network discovery framework necessitates the mitigation of the intruder node effect. The wormhole attack withinside the 6LoWPAN networks is decided through studying the common modifications in positive statistical patterns. Neighbor Watch System (NWS) contains an intruder against datagram-losing nodes in 6LoWPAN sensor networks prompted through black hole attacks. Neighbor Watch System detects the relaying node's misbehavior and makes use of less power than multipath frameworks. NWS applies a single-path data forwarding method looking for the relaying nodes. The data datagrams that

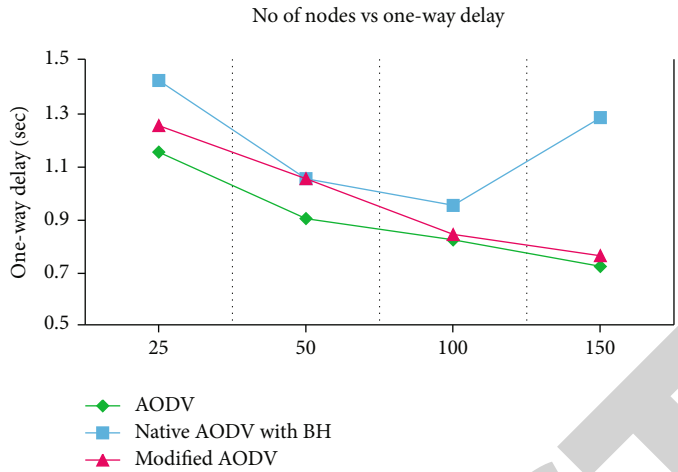


Figure 7: Compression of one-way delay.

transmit via intruder node may be dropped and outcome in low flow network rate. The manner of attack initialization and the rank assignment, in addition to the manner of nearby restore and data transmission, is given in Algorithm 2.

3.3. Local Repair Attack Implementation. The NETWORKS_IN_EVENT is initiated with the DIO message and its miles assigned with a completely unique rank; the use of the hash function is visible in Section 3.1. The rank and ID challenge exams, the preceding cost with inside the routing protocol table, and the modern values could be saved withinside the PREY_NODE_ID and PREY_NODE_RANK. The value assigned node is transmitted into the attacked region, and the attacked region repaired the use of the neighborhood restore workings or skip process is initiated to transmit the node to the end point node. The data transmission and the neighborhood restore is accomplished which is given in Algorithm 3.

A self-adaptive framework with 6LoWPAN local repair in AODV is illustrated in Figure 3. The nodes are deployed withinside the transmission networks, and the supply is initiated to transmit the data datagram to the end point. Every node is assigned with Node_ID and Rank with the help of the hash function. The supply node propagates the RREQ to the neighbor node to achieve the end point. The trouble happens because of the breakage of hyperlinks amongst the neighboring nodes N2 and N5. During data transmission, the nearby restore is initiated and the node N5 is abandoned. The node N2 initiates the RREQ on the nearby state to the node N10. The transmission is imitated with the aid of using the nearby restore workings. The breakage withinside the hyperlink is determined, and the reconstruction has begun out to transmit the data withinside the shortest path. The election framework is used to determine the best path to the end point node. The proposed framework maintains the hyperlink and transmits the data. The routing protocol desk is up to date with the neighbor listing for further data transmission. The whole proposed framework is represented in Figure 4.

4. Analysation of Simulation

In this part, the final results of the changed AODV with a neighborhood repair working are illustrated; this is in comparison with the AODV and native AODV with BH, the usage of a network simulator (NS-2). The research is done beneath parameters one-way delay and flow network charge with various nodes.

4.1. Flow Network Rate. Flow network rate is a fulfillment rate of data datagrams which are transmitted in a selected time and it is far signified in bits in keeping with second (bps) of the unit. The overall performance of changed AODV is investigated, and flow network rate is measured for numerous numbers of nodes. The yield high-flow network rate is attained withinside the changed AODV. This is proven in Table 1 and Figure 5. The flow network rate is compared for AODV, native AODV with BH, and modified AODV.

In Figure 5, a diagrammatic illustration of flow network rate evaluation is given, and from the statement, it is discovered that changed AODV yields for variety of nodes, respectively. The flow network rate of changed AODV is better than the AODV. When evaluated to native AODV with BH, the changed AODV yields for a variety of nodes, respectively. The flow network rate of the changed AODV is better than the native AODV with BH.

The flow network rate of AODV with black hole is in comparison with the prevailing algorithm specifically XMAC [21] and TBBT [22]. The simulation outcomes are given in Table 2, and the example of the end result is displayed in Figure 6. From the statement of the simulation analysis, it is diagnosed that the proposed algorithms display higher performance.

4.2. One-Way Delay. The routing protocol delay of the data datagram from the source node to end point throughout the transmission location is one-way delay. The delay in transmission affects the overall performance of the algorithm and the algorithm with minimal delay is the best algorithm.

One-way delay of the changed AODV is in comparison with existing algorithms particularly AODV and native AODV with black hole. The simulation outcomes are given in Table 3, and the example of the end result is displayed in Figure 7. From the remark of the simulation analysis, it is far recognized that the proposed algorithms display higher overall performance.

5. Conclusion

In this research article, a self-adaptive local repair framework for 6LoWPAN is proposed and the principle motive of the technique is to decorate the changed AODV network communication protocol for 6LoWPAN. Incidence of a sink hole attack and the overall performance elements, namely, one-way delay and flow network rate, are affected. Hence, identity and prevention of a sink hole with black hole attack is necessary. The proposed self-adaptive nearby repair framework can save you and enriches the overall performance of the AODV network communication protocol. The proposed framework minimizes the one-way delay and enriches the flow network rate. In the future, the network communication protocol may be changed for dense nodes, and the mobility framework additionally enriched with a brand new modification technique.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. Chalappuram, P. R. Sreesh, and J. M. George, "Development of 6LoWPAN in embedded wireless system," *Procedia Technology*, vol. 25, pp. 513–519, 2016.

[2] S. A. Awwad, C. K. Ng, N. K. Noordin, M. F. A. Rasid, and A. H. Alhawari, "Mobility and Traffic Adapted Cluster Based Routing Protocol for Terminal Node (CBR-Mobile) Network Communication Protocol in Wireless Sensor Networks," in *International Conference on Ad Hoc Networks*, pp. 281–296, Springer, Berlin, Heidelberg, 2010.

[3] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," *Network Working Group*, 2007.

[4] N. Halimatul, A. Ismail, and K. W. Ghazali, "A Study on Network Communication Protocol Stack in 6LOWPAN Model 1," *Network Working Group*, 2012.

[5] M. Rehenasulthana, P. T. V. Bhuvaneswari, and N. Rama, "Enhanced location based routing protocol network communication protocol for 6LoWPAN," 2012, https://arxiv.org/abs/1209.4778.

[6] M. Imran, F. A. Khan, T. Jamal, and M. H. Durad, "Analysis of detection features for wormhole attacks in MANETs," *Procedia Computer Science*, vol. 56, pp. 384–390, 2015.

[7] M. Mohanapriya and I. Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET," *Computers and Electrical Engineering*, vol. 40, no. 2, pp. 530–538, 2014.

[8] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 644–653, 2014.

[9] K. Manikannan and V. Nagarajan, "Optimized mobility management for RPL/6LoWPAN based IoT network architecture using the firefly algorithm," *Microprocessors and Microsystems*, vol. 77, article 103193, 2020.

[10] G. Glissa and A. Meddeb, "6LowPSec: an end-to-end security protocol for 6LoWPAN," *Ad Hoc Networks*, vol. 82, pp. 100–112, 2019.

[11] M. Mavani and K. Asawa, "Modeling and analyses of IP spoofing attack in 6LoWPAN network," *Computers & Security*, vol. 70, pp. 95–110, 2017.

[12] H. Fotouhi, D. Moreira, M. Alves, and P. M. Yomsi, "mRPL+: a mobility management framework in RPL/6LoWPAN," *Computer Network Communications*, vol. 104, pp. 34–54, 2017.

[13] P. Kaliyar, W. B. Jaballah, M. Conti, and C. Lal, "LiDL: localization with early detection of sybil and wormhole attacks in IoT networks," *Computers & Security*, vol. 94, article 101849, 2020.

[14] S. Deshmukh-Bhosale and S. S. Sonavane, "Design of intrusion detection system for worm hole attack detection in Internet of Things," in *Advanced Computing and Intelligent Engineering*, pp. 513–523, Springer, Singapore, 2020.

[15] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, Article ID 794326, 2013.

[16] S. Chakraborty and A. Majumder, "6LoWPAN security: classification, analysis and open research issues," *International Journal of Computational Intelligence & IoT*, vol. 1, no. 1, 2019.

[17] N. K. Sreelaja and G. A. Vijayalakshmi Pai, "Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks," *Applied Soft Computing*, vol. 19, pp. 68–79, 2014.

[18] A. Verma and V. Ranga, "Evaluation of network intrusion detection systems for RPL based 6LoWPAN networks in IoT," *Wireless Personal Network Communications*, vol. 108, no. 3, pp. 1571–1594, 2019.

[19] A. Le, *Intrusion detection system for detecting internal threats in 6LoWPAN [PhD. thesis]*, Middlesex University, 2017.

[20] G. Singh and J. Singh, "Prevention of black hole attack in wireless sensor networks using IPSec network communication protocol," *International Journal of Advanced Research in Computer Science*, vol. 4, no. 11, 2013.

[21] M. Buettner, G. V. Yee, E. Anderson, and R. Han, "X-MAC: a short preamble MAC network communication protocol for duty-cycled wireless sensor networks," in *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems - SenSys '06*, pp. 307–320, New York, NY, 2006.

[22] S. Sharma, S. Kumar, and B. Singh, "Routing protocol in wireless mesh networks: two soft computing based approaches," 2013, https://arxiv.org/abs/1307.3004.