Secure Intruder Information Sharing in Wireless Sensor Network for Attack Resilient Routing

Venkateswara Rao M[1]
Research Scholar
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundaion
Vaddeswaram,Andhra Pradesh, India

Srinivas Malladi[2]
Professor
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation,
Vaddeswaram,Andhra Pradesh, India

***Abstract*—Securing the routing process against attacks in wireless sensor network (WSN) is a vital factor to ensure the reliability of the network. In the existing system, a secure attack resilient routing for WSN using zone-based topology is proposed against message drops, message tampering and flooding attacks. The secure attack resilient routing provides a protection against attacks by skipping the routing towards less secure zones. However, the existing work did not consider the detection and isolation of the malicious nodes in the zone based wireless sensor network. To solve this issue, we proposed enhanced attack resilient routing by detecting malicious zones and isolating the malicious nodes. We proposed a three-tire framework by adopting sequential probability test to detect and isolate malicious nodes. Attacker information is shared in a secure manner in the network, so that routing selection decision can be made locally in addition to attack resiliency route selection provided at the sink. Overhearing rate is calculated for all nodes in each zone to detect blackhole attackers. Simulation results shows that the proposed Three Tier Frame work provides more security, reduced network overhead and improved Packet delivery ratio in WSNs by comparing with the existing works.**

Keywords*—Flooding; malicious zone; network overhead; overhearing rate; packet delivery ratio

I. INTRODUCTION

Wireless sensor network (WSN) technology is growing rapidly in many emerging sectors such as industry monitoring and control, home surveillance, wild life monitoring and smart farming. WSN is a network created by sensors equipped with wireless transceivers for communications. Sensor nodes collect environment parameters and send it to a central station for processing. The sensor node can send data to the central station in one hop or via multi hop forwarding depending on the distance between sensor node and the sink. Due to unattended nature and wireless infrastructure, the sensor network is easily susceptible to various kinds of attacks like message dropping, message tampering, message flooding etc. These attacks must be detected and mitigated to ensure the reliability of the sensor networks.

In [1] a secure attack resilient routing protocol is proposed to secure the routing process against possible attacks such as message dropping, message tampering and flooding. The whole network is divided into several zones and each zone is scored on the basis of the security and energy available in the zone. The zone with low security score is not preferred by the sink node for routing the packets. But this work did not specifically identify the malicious nature of the zone and did not isolate the specific attacker node. All zones are scored based on security and energy availability in that zone. Due to energy imbalance in the zones, still there is a higher chance of selecting less secure route by sink node.

It is important to identify the malicious zone and isolate the specific attacker node in that zone for secure data transmission. The attacker or compromised node may fabricate or tamper the data packet in the routing and it is a major problem to solve.

To solve this problem, a three-tier framework is proposed for secure attack resilient routing to transmit packets in secured manner from source node to destination node. The attacker node is detected and the information about the attacker node is shared in a secure manner in the network. Through sharing of attacker information, the network is made attack resilient and other innocent nodes are aware about the attacker node. Hence packets are routed only through innocent nodes in a secured manner.

Watch dog mechanism is employed by monitoring node in three tier frame work to detect the attackers. Monitoring node runs in promiscuous mode and observes all the packets within the zone. The monitoring node calculate overhearing rate (OR) for all nodes within its zone. Black hole attackers are identified Based on overhearing rate calculated by monitoring node. Sequential probability hypothesis test is used to check whether the Node is selective dropper or not. Monitoring node observes the rate of packets generated by the nodes in the zone and when rate exceeds certain threshold, it detects the node as flooding node.

Monitoring node shares the information about the message dropping and message tampering attackers to the sink in a secure way, so that sink can skip these routes while processing the packet for routing.

If monitoring node observes flooding attack from a node in a zone, it generates a blacklist packet containing the flooding node information. The packets from the blacklisted node are dropped by the nodes in the zone. Therefore, the effect of the flooding attack is restricted as much as possible.

The remaining part of the paper is organized as: The review of related work is presented in Section II. The

Proposed solution is elaborated in Section III. Detailed results are discussed with the help of tables and charts in Section IV. Conclusion and further enhancements for proposed work are depicted in Section V.

II. Related Work

Compromised nodes are detected using statistical analysis in [2]. Based on the past observations, sink calculates the probability for a node to be malicious. The overhead of detection is at sink. In [3], a light weight defense mechanism against black hole attack is proposed. Based on observation of packet sequence number, message droppers are identified. Once black hole message droppers are identified, ICMP control packets with information of black hole attackers is broadcasted in the network. So black hole nodes are skipped in the routing. Authors in [4] proposed a method to detect and alleviate from cooperative black hole attack. The detection of black hole is based on absence of consistent acknowledgement for the packets. The black hole node can be precisely located in this solution. The sensitive regions where there is high probability of packet loss are identified and routing through these paths is prevented using a sensitive guard procedure. E-watch dog mechanism is proposed in [5] to detect selective message droppers. This scheme is proposed to solve the problem of higher false positives in the traditional watch dog mechanism of packet monitoring. To solve the higher false positives in watch dog monitoring, the placement of monitoring hidden node problem is avoided. Time required for attacker detection, False positives, Network overhead and Accuracy of detection is measured for performance analysis. A heuristic solution for attack detection is proposed in [6]. In this work attackers are detected at the route discovery stage by observing the discrepancy in the sequence number of route request and route reply. Due to detection at route discovery stage, overhead for attack detection is less in this methodology. Black hole nodes are detected using cooperative sensing in [7]. A semi centric detection process called BlackDP is proposed in [8]. The solution can detect cooperative black hole nodes and isolate them in a two-stage process. In first stage any suspicious activity in the route reply with highest sequence number is notified to a cluster head. In the second stage, cluster head verifies all suspicious nodes and shares the information about blacklist to all nodes within the cluster to proactively drop the blacklisted nodes in the routing path. Authors in [9] proposed a solution to secure against cooperative black hole nodes in the MANET. Designated monitoring nodes are called security monitoring nodes and they are deployed in certain places in the network. Monitoring nodes detect black hole attackers by probing the packets and on detection of attack, the information is shared periodically to rest of the nodes. A cross layer protocol for detecting cooperative black hole nodes is proposed in [10]. The solution is based on watch dog monitoring of RTS/CTS at the MAC layer and to solve the problem of false alarm in watch dog monitoring, which is done by network layer. In [11], AODV protocol is extended for detecting multiple black hole attacks in the network. The black hole nodes are detected by monitoring the discrepancy in the count of packets. The node that detects the attacker, shares the attacker information to rest of the nodes in the network. The nodes maintain a dynamic blacklist to keep the information of black list nodes and proactively skip those black hole attackers from the routing path. A light weight black hole attack detection method is proposed in [12]. Cluster heads are deployed redundantly. Passive cluster heads use watchdog monitoring mechanism to detect compromised cluster heads. Authors in [13] proposed a black hole attack detection using acknowledgement scheme. Special designated nodes called monitor nodes are deployed in the network. Destination node sends an acknowledgement for each packet received from source node. This acknowledgement is monitored by monitoring node to detect packet loss due collisions. The traditional AODV protocol is integrated with bait detection scheme to detect collision attacks. On detection of black hole nodes, monitoring node forwards the information to rest of nodes to prevent blacklisted nodes from routing packets. Packet delivery ratio, Time required for attacker detection, False positives, Network overhead and Accuracy of detection is measured for performance analysis. Hidden Markov Model is applied for message drop attack detection in [14]. The nodes in the relay path are analyzed using Hidden Markov Model to detect the message drop attacks. Information about malicious nodes is sent to all other nodes in the network to mitigate the impact of such nodes in the routing path. A centralized geo-statistical hazard model to detect malicious regions in the network is proposed in [15]. Detection and mitigation of attacks is not handled uniformly in the network. Base station samples, analyze the suitability of the area for detection and launches detection only in the selected areas. A group-based technique for detection of multiple message drop attacker in the network is proposed in [16]. The clustering topology is used solution. The detection of message drop attack is done by the cluster head nodes. Cluster head nodes send probing messages to the nodes in the cluster and wait for acknowledgements. Based on acknowledgement monitoring, message droppers are detected and isolated in the network. Authors in [17] analyzed the recent trends in security of wireless sensor networks. Authors in [18] proposed analytical model for analyzing the security of wireless communications. Work in [19] and [20] identified malicious nodes and isolated them using certificate revocation. In addition to end-to-end delay, the propagation of large amount of data in MANETs is liable for higher energy usage, thereby influencing the parameters such as network efficiency, throughput, packet overhead, energy usage. To increase the longevity of the network and energy usage, efficient parameter metric measures are adopted in [21], [22].

III. Proposed Solution

A. Network Model

Each sensor node in WSN contains a unique ID. It is preconfigured with the private key of Hyperelliptic curve cryptography (HECC) and the corresponding public key is maintained at sink node. Hyperelliptic curve is a type of elliptic curves with genus ≥ 1. Elliptic curve cryptography (ECC) is found to have lower complexity than RSA. But still the complexity is high in ECC considering the case of resource constrained wireless sensor network. HECC is proposed to solve this problem. Equation (1) represents Hyperelliptic curve C with genus g over k.

$$C: y^2 + a(x)y = b(x) \quad (1)$$

Where

a(x): A polynomial with degree ≤ g over b

b(x): A monic polynomial with degree 2g+1 over b

Equation (2) is an example for sample HECC Function

$C: y^2 = x^5 - 5x^3 - 4x - 1$ over Q genus g=2. (2)

The public and private key pair of source node and sink is unique and not available to other nodes Also, the secret key sequence and a hash function H is assigned to each node in WSN. The secret key sequence and H is known to the source node and sink.

The whole WSN is split into $M \times M$ zones. The zone size is set in such a way that nodes in the same zone are one hop away from each other. For each zone, a node close to the center of the zone is selected as the monitoring node.

B. Secure Intruder Information Sharing

The architecture of secure intruder information sharing in WSN shown in Fig. 1.

A three tier frameworks is proposed to solve the secure intruder information sharing problem in wireless sensor networks.

- At the top tier is sink node, which prevents routing to risk zones and blocks the transition of Route Reply (RREP) containing risk zone relays.
- At the middle tier is the monitoring nodes [13]. They do not participate directly in routing, but instead passively monitor the packets and detect attacks within the zone and share this information to neighboring zones and sink.
- At the bottom tier is the ordinary sensor nodes and they send data through multi hop routing to the sink node.

There are two functionalities in the three-tier framework

- Detection of attack.
- Mitigation of attack.

1) Detection of attack: Watch dog mechanism is employed by the monitoring node to detect the attacks. Monitoring node runs in promiscuous mode and observes all the packets within the zone. The monitoring node calculate overhearing rate (OR) for all the nodes within its zone. The OR value is calculated by observing the RTS/CTS packets in the MAC layer using the Equation (3).

$$OR = \frac{TF}{TO} \quad (3)$$

Where TO is the count of overheard packet and TF is the count of forwarded packets? Every time monitoring node overhears packet TO is incremented and whenever monitoring node finds the overheard packet is forwarded TF is incremented. When the overhearing rate is continuously less than a threshold value, the corresponding node can be confirmed as black hole attacker.

But deciding on selective message dropper cannot be made based on OR threshold alone and monitoring node relies on sequential probability test to confirm the selective message dropper in this work. Sequential probability test is a statistical testing technique to check the validity of a hypothesis based on observation over a period of time.

Sequential probability test tries to prove one of the following hypotheses.

H_0: Node is not a selective dropper.

H_1: Node is a selective dropper.

To prove the hypothesis this work uses two thresholds A (upper) and B (lower) based on false positive rate α and false negative rate β [5] as shown in Equations (4) and (5).

$$A = \log \frac{\beta}{1-\alpha} \quad (4)$$

$$B = \log \frac{1-\beta}{\alpha} \quad (5)$$

The tolerant value for α, β is set by the monitoring node.

The log probability for a node x for T tests is given in

Equation (6)

$$P(x) = \log \frac{\prod_{t=1}^{T} P_1(S_t)}{\prod_{t=1}^{T} P_0(S_t)} \quad (6)$$

The following observations can be done Based on P(x).

Hypothesis H0 can be accepted if P(x)<A and the test can be stopped for the node x.

Hypothesis H1 can be accepted if P(x)>B and the test can be stopped for the node x. In this case, monitoring node marks the node as selective dropper.

For A<P(x)<B, both of the hypothesis cannot be confirmed now and further test is needed for node monitoring node observes the rate of packets generated by the nodes in the zone and when rate exceeds certain threshold, it detects the node as flooding node.

Monitoring node correlates the received and forwarded packets and checks if the packet content is altered. On detection of alteration of packets, the node which is forwarding can be identified as message tampering attacker.

Monitor node is able to detect message dropping, message tampering and message flooding attackers through the process of promiscuous monitoring.

2) Mitigation of attack: Monitoring node shares the information about the message dropping and message tampering attackers to the sink in a secure way, so that sink can skip these routes while processing the route reply (RREP).

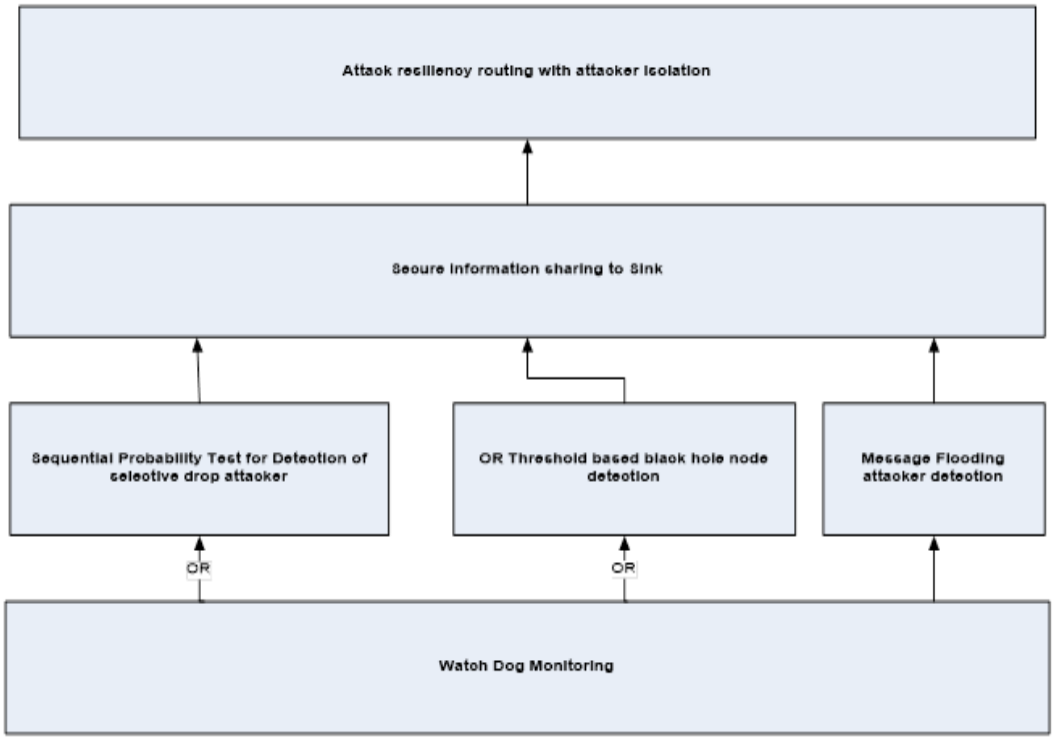

Fig. 1. Architecture of Secure Intruder Information Sharing.

Monitoring node sends the information of message dropper and message tampering attacker to sink node via a new packet type called blacklist. The blacklist packet has following format:

BlackList
{
Source
Timestamp
Encrypted payload
}

The encrypted payload has information of the attacker found. The encryption is done using HECC private key and sent to the sink. Encryption process is shown in Fig. 2.

If the packet is dropped in the zone, the monitoring node observes it and then attempts the cooperative forward for relaying the packet. Cooperative forwarding mechanism ensures the reliability of the BlackList packet.

Once the BlackList packet is received at sink, it decrypts the Encrypted payload using the HECC public key. The nodes found after decryption is added to a blacklist maintained at the sink. The Decryption process is shown in Fig. 3.

When RREQ is received at sink, before processing it for sending RREP sink checks the nodes in the RREQ for their presence in the blacklist maintained at the sink. In case of presence, RREP is not generated for the paths. Only from the rest of the paths, the one with highest security score is selected and RREP is generated with that path.

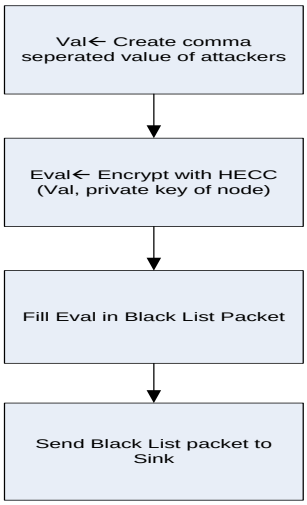

Fig. 2. Encryption Process.

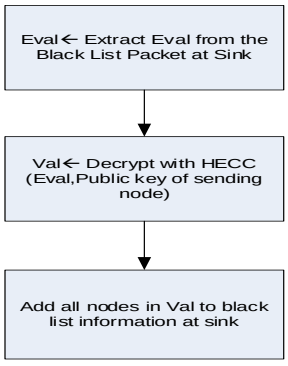

Fig. 3. Decryption Process.

In case monitoring node observes flooding attack from a node in a zone, monitoring node generates an ALERT packet containing the flooding node information. The ALERT packet is broadcasted to next immediate neighboring zones. The neighboring zone nodes and local zone nodes, after receiving ALERT packet, add the node in the ALERT packet to their blacklist. The packets from the blacklisted node are dropped by the nodes in the zone. Therefore, the effect of the flooding attack is restricted as local as possible.

3) Novelty in proposed solution: The proposed solution has better performance than the solutions reported in earlier works [5] and [13] in the following ways:

- Detection effort is localized within zone, thus reducing the unnecessary overhead.
- Mitigation is distributed in both sink and neighboring.
- Zones, thereby there is a more control on the attackers.
- Sharing of information between the zone and the sink is secured using HECC algorithm, thereby it is difficult to tamper the information about the attacker.
- A highly reliability for packet carrying attacker information is ensured.

IV. Results

Simulation was conducted in NS2 for proposed solution with the parameters shown in Table I.

The solution for proposed work is compared with solution proposed in [5] for selective attacker detection and solution proposed in [13] for detection malicious attacker in sensor network.

In terms of the following parameters, the performance of the proposed and existing works is compared.

- Packet delivery ratio
- Accuracy of detection
- False positives
- Time for attack detection
- Network Overhead

The ratio of number of packets received at sink to the number of packets sent from source to sink is termed as packet delivery ratio. The rationale for measuring the packet delivery ratio is to measure the resilience of the packet transmission in the network in presence of message dropping attacks.

The packet delivery ratio is calculated by varying the number of nodes with 10% of nodes as attackers and the result is presented Table II and plotted Fig. 4.

The packet delivery ratio in the proposed work is 7.65% more than that of [5] and 8.72% more than that of [13].

The packet delivery ratio is measured for fixed 250 nodes in the network and by varying the attack rate from 5% to 20% and the result is shown in Table III and plotted in Fig. 5.

TABLE I. Parameters of Simulation

Parameters	Values
Number of Nodes	50 to 250
Transmission range(m)	100
Simulation area(m^2)	1000*1000
Node propagation	Random
Span of Simulation (minutes)	30
Queue Size of Interface	50
Medium Access Control	802.11
Percentage of attackers	10% of total nodes

TABLE II. Packet Delivery Ratio

No of Nodes	Proposed	[5]	[13]
50	88.4	82.15	81.5
100	90.2	83.34	82.17
150	91.5	84.56	83.11
200	92.7	85.12	84.32
250	93.6	86.31	85.5

Fig. 4. Packet Delivery Ratio.

TABLE III. Packet Delivery Ratio based on Attack Percentage

Percentage of attacker	Proposed	[5]	[13]
5	96.4	88.15	87.5
10	93.6	86.31	85.5
15	91.5	84.56	83.11
20	90.7	83.12	82.32

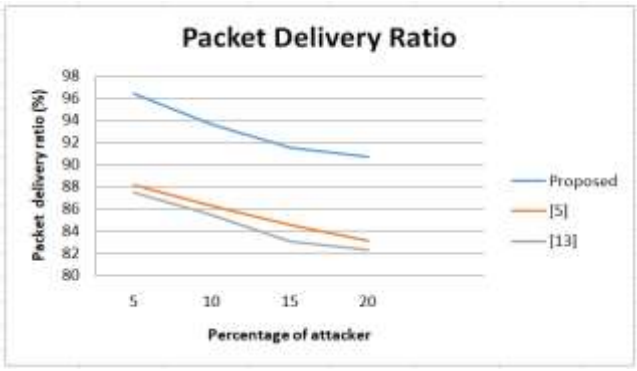

Fig. 5. Packet Delivery Ratio based on Attack Percentage.

In WSN, the packet delivery ratio decreases as the attack rate increases. But the packet delivery ratio is still higher in the proposed solution. It is 8.07% higher compared to [5] and 9.08% higher compared to [13].

The accuracy of attack detection is measured by varying the number of nodes with 10% of nodes as attacker and the result is presented in Table IV.

The attack detection ratio in the proposed solution is 7.72% higher compared to [5] and 8.82% higher compared to [13]. The reason for increased attack detection ratio is due to localization of detection to zone level in the proposed solution.

False positives are very common in any detection technique. Certain drops due to network conditions could be wrongly misinterpreted as message dropping attack. False positives are measured by varying the number of nodes with 10% of nodes as attacker and the result is given in Table V and Fig. 6.

The false positives in the proposed work is 28% lower compared to [5] and 18.3% lower compared to [13]. The reason for reduced false positives it due to better watch dog mechanism with localized monitoring and sequential probability test in the proposed solution.

TABLE IV. ACCURACY OF ATTACK DETECTION

No of Nodes	Proposed	[5]	[13]
50	90.4	83.25	82.5
100	91.4	84.44	83.17
150	92.5	85.51	84.11
200	93.6	86.15	85.32
250	94.5	87.33	86.5

TABLE V. FALSE POSITIVES

No of Nodes	Proposed	[5]	[13]
50	10.4	13.65	12.5
100	11.5	14.54	13.17
150	12.2	15.61	14.71
200	13.3	16.75	15.82
250	13.8	17.83	16.2

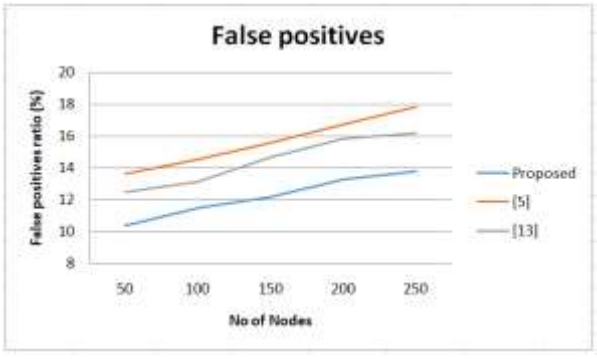

Fig. 6. False Positives.

Time for detection of attack is measured for a fixed node of 250 by varying the percentage of attacks and the result is given in Table VI and Fig. 7.

The time for detection of attack is almost flat with only a slight increase in the time compared to [5] and [13]. This is because of parallelization is detection at zone level.

The network overhead is calculated for a fixed node of 250 by varying the percentage of attacks and the result is given Table VII and Fig. 8.

TABLE VI. ATTACK DETECTION TIME

Percentage of attacker	Proposed	[5]	[13]
5	11	13	12
10	12	15.54	14.17
15	12.5	17.61	16.71
20	12	20.75	18.82
25	12.8	22.83	21.2

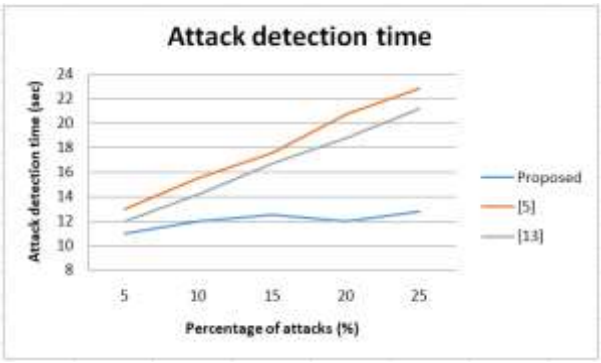

Fig. 7. Attack Detection Time.

TABLE VII. NETWORK OVERHEAD

Percentage of attacker	Proposed	[5]	[13]
5	8	13	12
10	11	15	14
15	15	18	17.2
20	19	22	21
25	22.5	24	23.2

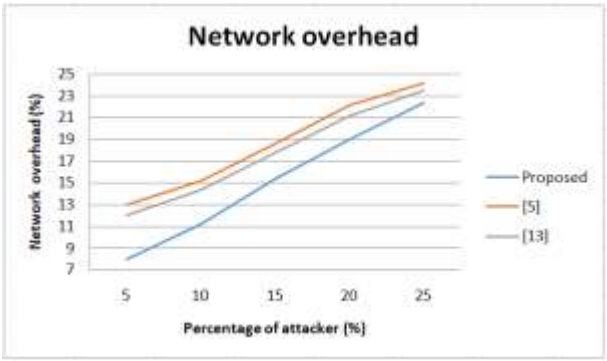

Fig. 8. Network Overhead.

The network overhead in the proposed work is 22.52% lower compared [5] and 17% lower compared to [13]. The proposed solution has lower overhead because of the distributed nature in the proposed solution and attack influence is localized.

V. Conclusion and Future Work

In this work, a secure intruder information sharing in wireless sensor network for attack resilient routing is proposed. The proposed solution is able to detect message drop, message tampering and message flooding attacks with higher accuracy when compared to existing solutions. The malicious node is identified and isolated in the zone. Also due to attack detection localization with zones, the network overhead and time to detect attack is comparatively lower in the proposed solution. The information about the attacker is shared in a secure manner using HECC and there is higher reliability for attacker information sharing in the network.

Due to unattended node deployment batteries may have limited power which requires additional resources to recharge.

As part of the future work, the proposed work can be extended to increase communication range in secured manner with Realtime scenario by considering collision avoidance and energy constraints.

References

[1] Venkateswara Rao M and Srinivas Malladi, “Secure Energy Efficient Attack Resilient Routing Technique for Zone based Wireless Sensor Network” International Journal of Advanced Computer Science and Applications (IJACSA),11(12),2020.http://dx.doi.org/ 10.14569 / IJACSA.2020.0111267.

[2] Stefanos A. Nikolidakis, Dimitrios D. Vergados, Christos Douligeris Algorithms, Energy Efficient Routing in Wireless Sensor Networks Through Balanced Clustering, 2013.

[3] J. Jiang, Y. Liu and B. Dezfouli. (2018): A Root-based Defense Mechanism Against RPL Blackhole Attacks in Internet of Things Networks, Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), Honolulu, HI, USA, 2018,pp.1194-1199,doi:10.23919/APSIPA. 2018.8659504.

[4] M.Rajesh Babu,S. Moses Dian, Siva Chelladurai, Mathiyalagan Palaniappan(2015) : Proactive Alleviation Procedure to Handle Black Hole Attack and Its Version, The ScientificWorld Journal, vol.2015,ArticleID 715820,11 pages, 2015. https://doi.org/10.1155/2015/715820.

[5] Zhang, Qiong & Zhang, Wenzheng. (2019). Accurate detection of selective forwarding attack in wireless sensor networks. International Journal of Distributed Sensor Networks. 15. 155014771882400. 10.1177/1550147718824008.

[6] Rutvij H. Jhaveri and Narendra M. Patel,"A sequence number based bait detection scheme to thwart gray hole attack in mobile ad hoc networks”, Wireless Network, Springer, 2015, Vol.21, Issue 8, pp.2781-2798.

[7] Y M. Khamayseh,ShadiA,Aljawarneh, and Alaa Ebrahim Asaad, “Ensuring Survivability against Black Hole Attacks in MANETS for Preserving Energy Efficiency”, Sustainable Computing: Informatics and Systems. Vol.18, pp.90-100, suscom.2017.07.001 http://dx.doi.org/ 10.1016/j.

[8] S. S. Albouq and E. M. Fredericks.(2017): Lightweight Detection and Isolation of Black Hole Attacks in Connected Vehicles, IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), Atlanta, GA, 2017, pp. 97-104, doi: 10.1109/ICDCSW.2017.23.

[9] T. Poongodi and M.Karthikeyan ,"Localized Secure Routing Architecture Against Cooperative Black Hole Attack in Mobile Ad Hoc Networks", Wireless Personal Com.,Springer,2016.Vol.90, Issue 2, pp.1039-1050.

[10] R. Baiad, H. Otrok, S. Muhaidat and J. Bentahar. (2014) :Cooperative cross layer detection for blackhole attack in VANET-OLSR, International Wireless Communications and Mobile Computing Conference (IWCMC), Nicosia.

[11] Hamamreh, Rushdi. (2018). Protocol for Multiple Black Hole Attack Avoidance in Mobile Ad Hoc Networks. 10.5772/intechopen.73310.

[12] Ismail,Asima & Amin, Rashid. (2019). Malicious Cluster Head Detection Mechanism in Wireless Sensor Networks. Wireless Personal Communications. 108. 10.1007/s11277-019-06512-w.

[13] Terence,Sebastian& Purushothaman, Geethanjali. (2019). A novel technique to detect malicious packet dropping attacks in wireless sensor networks. Journal of Information Processing Systems. 15. 203-216. 10.3745/JIPS.03.0110.

[14] Wazid, Mohammad & Katal, Avita & Sachan, Roshan & Goudar, R.H. & Singh, Dharam. (2013). Detection and prevention mechanism for Blackhole attack in Wireless Sensor Network.576-581. 10.1109/iccsp.2013.6577120.

[15] Shafiei, Hosein &Khonsari, Ahmad & Derakhshi, Hazhir & Mousavi,P..(2014). Detection and mitigation of sinkhole attacks in wireless sensor networks.Journal of Computer and System Sciences.80.644–653.10.1016/j.jcss.2013.06.016.

[16] Wazid, Mohammad & Das,Ashok Kumar. (2016). A Secure Group-Based Blackhole Node Detection Scheme for Hierarchical Wireless Sensor Networks. Wireless Personal Communications.94.10.1007/s11277-016-3676-z.

[17] Manjunath, B. E., and P. V. Rao. "Trends of Recent Secure Communication System and its Effectiveness in Wireless Sensor Network." Journal of Innovation in Electronics and Communication Engineering 6.2 (2016): 46-52.

[18] Dr. P.V.Rao, Manjunath B E, “Unique Analytical Modelling of Secure Communication in Wireless Sensor Network to Resist Maximum Threats”, International Journal of Advanced Computer Science and Applications, (IJACSA) Vol. 10, No. 2, pp 421-427, 2019.

[19] Chowdary, Krishna, and K. V. V. Satyanarayana. "MALICIOUS NODE DETECTION AND RECONSTRUCTION OF NETWORK IN SENSOR ACTOR NETWORK." Journal of Theoretical & Applied Information Technology 95.3 (2017).

[20] Vamshi krishna, H., & Swain, G. “Identification and avoidance of malicious nodes by using certificate revocation method.” International Journal of Engineering and Technology (UAE), 7(4.7 Special Issue 7) (2018).

[21] Prasad,A.Y.,and Balakrishna Rayanki."A generic algorithmic protocol approaches to improve network life time and energy efficient using combined genetic algorithm with simulated annealing in MANET." International Journal of Intelligent Unmanned Systems (2019). Vol. 8 No. 1, pp. 23-42.

[22] Prasad,A.Y.and R.Balakrishna. "Implementation of optimal solution for network lifetime and energy consumption metrics using improved energy efficient LEACH protocol in MANET." Telkomnika Vol. 17 No.4 (2019): 1758-1766.