Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.778162

ENHANCING QOS IN WSN THROUGH ADAPTIVE REGIONAL TRANSMISSION APPROXIMATION-BASED BLACK HOLE ATTACK DETECTION

Mrs. A. Rukmani
Research Scholar, PG & Research Department of Computer Science,
Government Arts College (Autonomous), Karur – 639005, Tamilnadu, India
(Affiliated to Bharathidasan University, Thiruchirappalli-24)

Dr. C. Jayanthi
Associate Professor, PG & Research Department of Computer Science,
Government Arts College (Autonomous), Karur – 639005, Tamilnadu, India
(Affiliated to Bharathidasan University, Thiruchirappalli-24)

Abstract:

The problem of black hole attack detection in Wireless Sensor Network has been well studied. Presence of malicious node at the transmission path encourages the threat and degrades the performance of entire network. To handle this, an efficient Adaptive Regional Transmission Approximation (ARTA) approach is presented in this article. The method focused to detect the presence of black hole attack at data transmission by approximating the traffic and throughput parameters in the region considered. The method works based on different parameters like energy, location, transmission history, and other regional parameters. According to the above mentioned parameters, the method approximates the trust of different nodes in region manner. The node approximation is performed by measuring Route Trust (RoT) and the regional nodes are approximated with Regional Trust Measure (RTM). Based on these two trust measures computed, the method performs black hole attack detection. The proposed ARTA algorithm produces higher performance in black hole attack detection with less time complexity.

Index Terms: WSN, Black hole attack, Regional Approximation, ARTA, RoT, RTM, trust evaluation, QoS.

1. Introduction:

Wireless sensor network (WSN) has been identified as dominant in the field of communication as the way it supports the telecommunication worlds in several ways. As it can be deployed in rapid way and supports the access of various services, many organizations itself deployed such networks. Anyway, it is a collection of set of sensor nodes, which comes with limited bound of energy and transmission ratio. This restricts the sensor node in performing data transmission in direct way. So that, the sensor nodes involve in cooperative transmission with the intermediate nodes. This opens the gate for the malicious node to perform any threat.

Any network is subject to face many threats and WSN is not an exemption for network threats. There are number of threats can be named which are generated by different malicious nodes. Some of the nodes involve in packet drop by eaves dropping and some of them involve in selective drop and selective forwarding. Also the malicious nodes would involve in modification attack which modify the data in the packet and forward them. In this way, black hole attack is the one which has been generated by the malicious nodes of the network, which in turn update the packet data or send malicious information about the route after tunneling the network stream through the malicious node. It would try to get participate in all the transmission and tunnel the packet to some of the malicious node which in turn damage the network transmission by performing different threats.

There are number of approaches available to handle black hole attack. In general, the malicious node tunnel the stream by participating in the almost all the transmission. The malicious node has been get selected by the source only based on the energy and hop count parameters. Because, the source node would always look for a shortest hop route and energetic one. If there is a neighbor having route to reach the destination, then it would select the node. In this way, the malicious node would claim that it has the short route and more energy constraints at the time of route discovery. This makes the source to select the malicious node as the forwarding node. So that it is necessary to verify the trust of the source node before selecting forwarding the data packets.

The verification process can be done in several ways. First, the nodes trust can be measured based on the completeness of the transmissions done through the particular node. Another on is by collecting the votes from the neighbors. Also, we can infer the trust of node by analyzing the physical parameters like location verification, energy analysis and topology of the network. However, the existing approaches are not obtaining the expected performance in detecting the blackhole attack. This encourages the author in designing an adaptive approach to handle this problem.

Towards the scope, an efficient adaptive Regional Transmission Approximation based black hole attack detection scheme is presented. The method not just analyzes the physical parameters but also analyze the topology constraints, traces of previous transmission. By analyzing multiple features and constraints, the presence of malicious node not alone identified, it would identify the region where the malicious nodes are located which would help to divert the entire data transmission to other regions and can avoid such regions. This would greatly support the increase of network performance. The detailed approach is discussed in the next sections.

2. Related Works:

There are number of approaches available to handle the problem of black hole attack. Around this, a set of approaches are analyzed and presented in this section.

(Baviskar B.R, Patil V.N, 2014) Propose an efficient technique that uses multiple base stations deployed in the network to counter the impact of black holes on data transmission, using java simulator and performance compare with multiple base station and without multiple base station to prevent black hole attacks. It implemented using Net bean IDE Java network simulator .

(Wang Chun-Hsin and Li Yang-Tang 2013) proposed a new method to detect malicious nodes actively. Without modifying or adding routing protocols, only few pairs of detection nodes are needed, which can identify and isolate malicious nodes.

(Mehdi Medadian, et. al 2009) an approach is proposed to combat the Black hole attack by using negotiation with neighbors who claim to have a route to destination.

(Wazid Mohammad, et. al 2013) An algorithm named as Topology Based Efficient Service Prediction (TBESP) algorithm has been proposed depending upon the analysis done which will help in choosing the best suited topology as per the network service requirement under blackhole attack.

(Tiwari Mukesh, et. al 2009) introduces a specification based intrusion detection system for wireless sensor networks.

(M. Tokala and R. Nallamekala, 2018) propose LISA algorithm along with Steiner Minimal Tree algorithm to route data in a Secured manner. LISA algorithm provides both confidentiality and integrity to data.

(B. Patil and R. Kadam, 2018) proposed secure and trustable routing technique with utilizing multi data flow topologies (MDT) scheme to defend against this attack and proposed a suite of optimization methods to minimize the energy cost while keeping the system's security in a sufficient level. (F. Mezrag, et. al 2017) proposes a new secure protocol based on the well-known LEACH routing protocol named Hybrid Cryptography-Based Scheme for secure data communication in cluster-based WSN (HCBS). As a multi-constrained criteria approach, HCBS is built on a combination of the cryptography technique based on Elliptic Curves to exchange keys that uses symmetric keys for data encryption and MAC operations.

(C. Deepa and B. Latha, 2018) proposes an inter and intra cluster head selection method which consumes less energy and increase the network lifetime. To achieve the security, we introduce elliptic curve cryptography at the cluster head level.

(R. Shukla, et.al 2017) enhances security of Trust and energy aware secure routing protocol (TESRP) by securing it against wormhole attack. TESRP is one of the best trust based protocol but this protocol does not provide security from wormhole attack. Trust algorithm together with sequence number concept has been used for securing TESRP from wormhole attack. (G. Liu, et. al 2018) (ESRQ) propose a lightweight and efficient security routing method by combining the trust mechanism with q-learning algorithm. The sensor node determines the credibility of the specific node autonomously and efficiently according to the performance of the behavior of the node.

(HIlmi Lazrag, 2016) present a game theoretic approach for routing with the purpose of optimizing energy consumption while using a security layer. To achieve this goal we propose an algorithm which control the transmission power, balance the load traffic and secure the interactions using elliptic curves digital signature (ECDSA). (M. Kavitha, 2017) presents an efficient city energy management system with secure routing is developed to minimize the energy consumption, maintain the load in the peak hours and reduce the cost based on the TOU tariff. This helps to enhance the OREM scheme. . With the help of a modified dynamic source routing with adaptive local routing protocol routing (MDSR-ALR) protocol, misrouting paths are identified in wireless sensor network.

(Hanane Kalkha, et. Al 2019) presents a Hidden Markov model (HMM) based black hole attack detection scheme towards WSN. The method selects a shortest path to avoid malicious node path. (Ganesh R. Pathak,. Et al 2020) presents a secure AODV is designed to handle black hole attack in WSN. The Enhanced Detection and Prevention Mechanism for Black Hole Attack (EDPMBA) Method of Trust which detects the Black Hole attack in the network which uses attacker detection metric.

(M. M. Ozcelik, 2017) present a hybrid trust based intrusion detection scheme where each sensor node computes functional reputation values for its neighbors by observing their activities. Base Station (BS) detects malicious nodes by combining functional reputation values and misuse detection rules.

(Z. Sun, et. al 2018) design a three level detection mechanism by taking the advantage of the cooperation of the base station, detection nodes, and ordinary nodes considering their different capabilities, and to modify the V-detector algorithm by modifying the detector generation rule and optimizing the detectors, and to use the principal component analysis to reduce the detection features.

(V. T. Alaparthy and S. D. Morgera, 2018) a multi-level intrusion detection system (IDS) is designed based on the functions of various immune cells. This is realized by monitoring WSN parameters, such as energy, volume of data and frequency of data transfer and developing an output based on their weights and concentrations which is a suitable basis for IDS design in WSNs.

(Higo Pires, 2017) present a agent based framework for intrusion detection in wireless sensor networks and describes the proposal of a framework for intrusion detection in WSNs based on intelligent agents.

(Christiana Ioannou, 2018) propose mIDS, which monitors and detects attacks using a statistical analysis tool based on Binary Logistic Regression (BLR). mIDS takes as input only local node parameters for both benign and malicious behavior and derives a normal behavior model that detects abnormalities within the constrained node.

(Adwan Yasin and Mahmoud Abu Zant, 2018) presents enhanced AODV by integrating a new lightweight technique that uses timers and baiting in order to detect and isolate single and cooperative black-hole attacks.

(AnkitKumar, Vijayakumar Varadarajan, 2021) a secure AODV routing protocol is developed for detection of black hole attack in this paper. The proposed method is a modified version of the original AODV routing protocol with improvements in the RREQ packet and RREP packet protocols. For added security, a cryptography function-based encryption and decryption is included to verify the source and destination nodes.

All the above discussed methods suffer to achive higher performance in black hole attack detection.

3. Adaptive Region Transmission Approximation Based Black hole Attack Detection:

The proposed adaptive region transmission approximation algorithm works in two phases. It analyzes the trust of neighbors as well as analyses the trust of regional nodes as well. To perform this, at the data transmission, the node collects the route by performing route discovery and collects the nodes transmission history. Using the feature of the history of different nodes, the method analyzes the trust of neighbors based on two factors like physical trust and transmission trust. Based on the result of both of them, the method identifies the route or neighbor through which the data transmission has been performed. On the other side, the method analyzes the trust of the region by approximating the transmission outcome of region through which the set of transmissions carried. Based on the result of both the analysis, the method selects a optimal route to perform transmission as well as identify the region where malicious nodes are present and the neighbor which is a malicious node. Identified data has been propagated for the other trusted neighbors to carryout secure data transmission. The detailed approach is presented in this section.

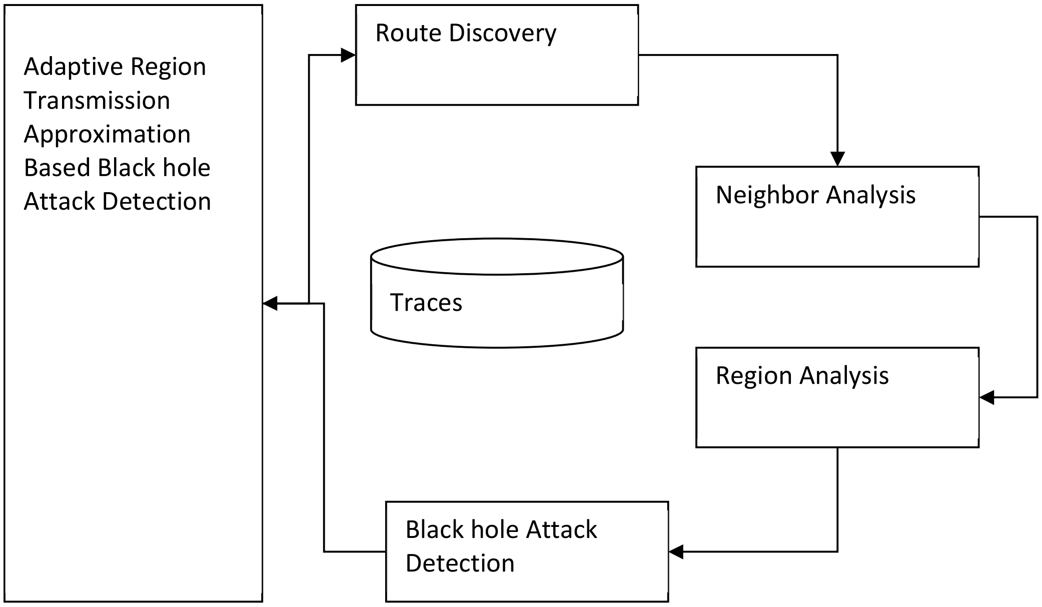
Adaptive Region Transmission Approximation Based Black hole Attack Detection
Route Discovery
Neighbor Analysis
Traces
Region Analysis
Black hole Attack Detection

Figure 1: Architecture of Proposed ARTA Model

The functional architecture of proposed ARTA black hole attack detection model has been presented in Figure 1, and the functional components are detailed in this section.

3.1 Route Discovery:

Route discovery is the process of discovering set of routes between any two node. Here, the source node perform this process by generating ARTA_RREQ packet which has the source node and destination node id. Generated packet has been broadcasted in the network which has been received by the neighbors of the source. The neighbors verifies the availability of any link to reach the destination node. If there is a route to reach the destination then it has been sent to the source through the ARTA_RREP message. Otherwise, the neighbor performs multicast to the neighbors other than the source from where the packet has been transmitted. In this approach, the route reply has been transmitted with the details containing the location of the node, number of transmission it has done, and its energy value. The source node fetches these information from the reply message and updates the node table. Discovered routes and information are used towards black hole attack detection.

Algorithm:

```
Input: Packet P, Route Table RT, Node Table NT, Neighbor Table NeT
Output: Route Table RT, Node Table NT, Neighbor Table NeT
Begin
    Read P, RT, NT, NeT
```

```
              $size(RT)$
    If $RT(i) \rightarrow P.Destination$ then
               $i = 1$
          Transmit the packet to the destination
    else
          Generate ARTA_RREQ {Source Node ID, Destination ID}
          Broadcast packet in the network.
          Neighbor receives ARTA_RREQ packet.
          If has route to Destination
                Generate ARTA_RREP{Route R, Node.location, energy, NoTr}
                Send to source
          Else
                Multicast the ARTA_RREQ to neighbors
          End
    End
    Source Receives the ARTA_RREP packet.
    Extract Route R = $Route \in ARTA\_RREP$
    Add to Route table RT = $\sum$(Routes $\in$ RT) $\cup$ R
    For each route R
          Extract node features NF = {Node ID, Location, Energy, NoTr}
          Add to node table NT.
    End
Stop
```

The above discussed algorithm represents how route discovery has been performed to support data transmission as well as handling black hole attacks. The method discovers the routes as well as nodes features to support the attack detection process.

3.2 Neighbor Analysis:

Neighbor analysis is the process of analyzing the trustworthy of neighbors in handling the data transmission. The trust of the neighbors is analyzed in two different ways, one in terms of physical trust and another in terms of transmission trust. The physical trust represents the genuine of any node which has been measured based on the location parameters and transmission range. Because, the node would mention that it has the shortest route to reach the destination, but by measuring the physical trust of the node, the possibility of the node having said shortest route can be identified. Similarly, in terms of transmission trust, the trust of the node can be measured according to the number of transmission, energy and so on. Because, by analyzing the above mentioned features, we can identify whether the node is genuine or not. . To perform this, at the data transmission, the node collects the route by performing route discovery and collects the nodes transmission history. Using the feature of the history of different nodes, the method analyzes the trust of neighbors based on two factors like physical trust and transmission trust. Based on the result of both of them, the method identifies the route or neighbor through which the data transmission has been performed.

Algorithm:

Input: Route Table RT, Neighbor Table NeT, Node Table NT, Neighbor N

```
Output: Route Trust RoT
Start
    Read RT, NeT, NT.
    For each route R
        Compute physical trust PT = $\frac{Dist(R.N.Location-Destination.Location)}{R.Hop}, \times X(if < N.TransmissionRange, 1,0 \times if(R.hopcount < \frac{\sum_{i=1}^{size(RT)} Hopcount(RT(i))}{size(RT)})?0:1$
        Compute Transmission Trust TT = $\frac{NeT(i).NodeID==R.N,\ \underset{i=1}{\overset{size(NeT)}{Dist(\ (\mu\times R.N.NoT),Node.Energy)}}<R.N.Energy?1:0}{1}$
        Compute Route Trust RoT = PT×TT
    End
Stop
```

The above discussed algorithm represents how the neighbor analysis is performed to measure the trust of neighbors towards route selection. The method estimates the physical trust and transmission trust to compute the value of route trust, where route trust value has been used to perform black hole attack detection.

3.3 Region Analysis:

The region analysis procedure performs the analysis of trust according to the transmission history of nodes located in the region. To measure this, the method first split the entire network into number of region and for each region, the set of nodes located are identified. Now, for each region, set of transmission happening is identified and computed. Similarly, the method computes the transmission rate for different regions. Now, the method identifies the destination id of different transmission. Using the transmission rate towards various destination, the method identifies estimates the transmission rate for various regions. Using both of them, the method computes the region trust measure (RTM). Estimated RTM value has been used to perform black hole attack detection.

Algorithm:

```
Input: Network Topology NeTo, Transmission History Th, Region R, Destination D
Output: RTM.
Start
    Read NeTo, Th, R.
      Region set Rs = Split(NeTo, 8)
    Identify node set Ns = $\sum_{i=1}^{size(R)} Nodes \in R(i)$
        For each node Ni
            Identify Transmission list Tlist =
            $\sum_{i=1}^{size(Th)} Th(i).Route.Ni \in N \ \&\&\ Th(i).Dest == D$
        End
        Compute  transmission rate TR = $\sum_{i=1}^{size(NS)} Size(NS(i).Tlist) \big/ size(NS)$
        For each other region OR
            Compute Transmission Rate TR.
        End
        Compute average transmission rate ATR = $\sum TR \big/ size(RS) - 1$
        Compute Region Trust Measure RTM = TR(R) × (TR( R) <ATR ? 1:0)
Stop
```

The above discussed algorithm represents how region analysis is performed. The method estimates the transmission rate and average transmission rate for different region nodes. According to the value, the method computes the value of Region Trust Measure. Estimated value of RTM is used to perform black hole attack detection.

3.4 Black Hole Attack Detection:

The proposed approach performs black hole attack detection by analyzing the network and neighbors and regions for their trust. The method first performs the route discovery to detect the set of available nodes and to get details of nodes about their energy, number of transmission involved, energy and so on. Using them, the method first performs neighbor analysis and computes Route Trust (RoT) and second analyze the region of the network to compute Region Trust Measure (RTM). Using both the values, the method computes the Forwarding trust (FT) to decide the trust of the region for data transmission. If the RTM value of any region is identified with the value of 0, then it has been identified as the region has malicious nodes and not suitable for data transmission. Based on the forwarding trust value, the method selects optimal region and node to perform data transmission.

Algorithm:

```
Input: Node Table NT, Route Table RT, Trace history Th.
Output: Null
Start
    Read NT, RT, Th
     Region set Rs = Split(NeTo, 8)
    For each region R
        RTM = Perform Region Analysis
        If RTM==0 then
            Malicious nodes are there.
        End
    End
    Region R = Choose maximum RTM region.
    Perform Neighbor Analysis.
    Choose route with maximum trust.
    Perform data forwarding.
Stop
```

The above discussed algorithm shows how the neighbor and region analysis is performed. According to the result of both analysis, the method performs route selection and black hole attack detection. Selected route has been used to perform data transmission.

4. Results and Discussion:

The proposed adaptive Regional Transmission Approximation Based Black hole Attack Detection scheme is presented in this paper. The method has been implemented and evaluated for its performance under various circumstances. The results obtained are compared with the results of other approaches.

Key	Value
Platform	Network Simulator 2
Total sensors	200
No of Adversaries	10
Time	15 Minutes

Table 1: Simulation Details

The conditions considered for the performance evaluation of proposed approaches has been measured and presented in Table 1. The methods are evaluated for their performance under different factors as follows:

Black hole Attack Detection Accuacy %			
	50 Nodes	100 Nodes	200 Nodes
TSR-ActiveTrust	67	72	75
JDICA	70	75	78
EDPMBA	74	78	83
ARTA	82	86	92

Table 2: Analysis on Black hole Attack Detection Accuracy

The performance on security provided in routing is measured for different methods at different number of nodes in the network. In each case the proposed ARTA approach has produced efficient results in the ratio 82%, 86% and 92%in the conditions of 50 nodes, 100 nodes and 200 nodes conditions.

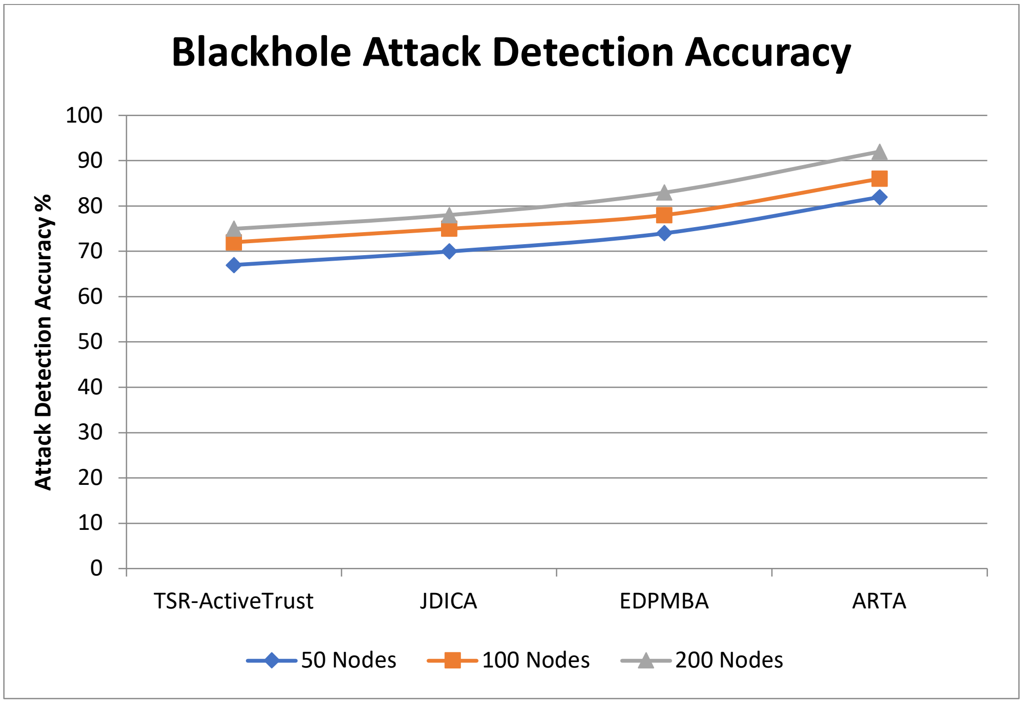

Figure 2: Comparison on security performance

The performance on security provided in routing is measured for different methods at different number of nodes in the network. In each case the proposed ARTA approach has produced efficient results.

Latency Ratio			
	50 Nodes	100 Nodes	200 Nodes
TSR-ActiveTrust	38	34	31
JDICA	36	32	29
EDPMBA	31	28	25
ARTA	28	25	21

Table 3 Analysis on Latency Ratio of STABD

The value of latency produced by different methods in transmitting the packets are measured and presented in Table 3. In each case the proposed ARTA approach has produced less latency compare to other methods. The proposed method has produced latency in the ratio of 28, 25, and 21 seconds in the conditions of 50, 100 and 200 nodes in the network.

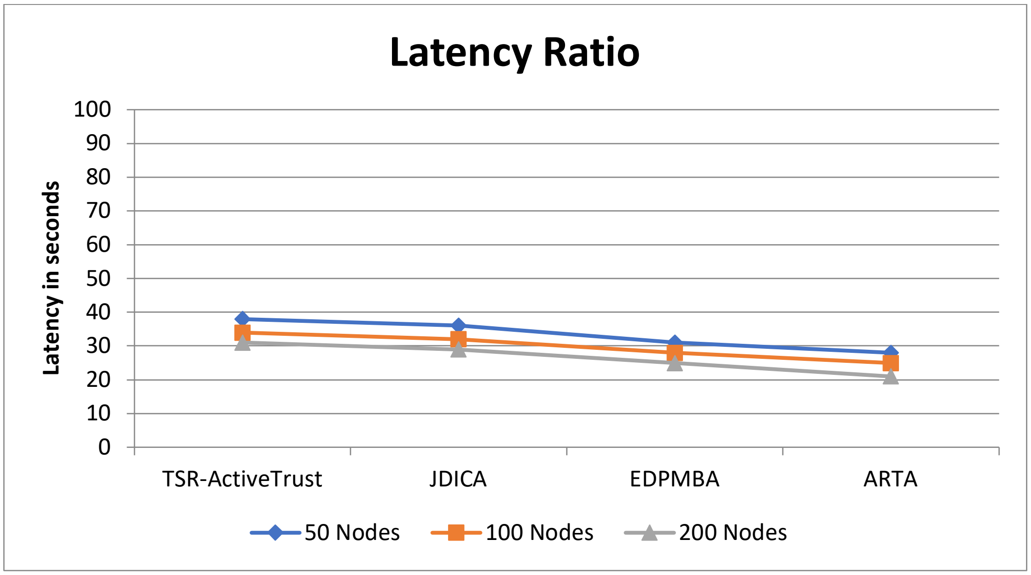

Figure 3: Comparison on latency ratio of STABD

The value of latency produced by different methods in transmitting the packets are measured and presented in Figure 3. In each case the proposed ARTA approach has produced less latency compare to other methods.

Throughput Performance %			
Method	50 Nodes	100 Nodes	200 Nodes
TSR-ActiveTrust	68	72	77
JDICA	73	77	82
EDPMBA	77	81	86
ARTA	81	84	89

Table 4: Analysis on Throughput Performance

The performance introduced in throughput factor by different methods are measured and presented in Table 4. It has been measured by varying the number of nodes in the simulation as 50 nodes, 100 nodes and 200 nodes. The proposed ARTA scheme has achieved throughput performance in the ratio 81%, 84 and 89% which is higher than the other approaches.

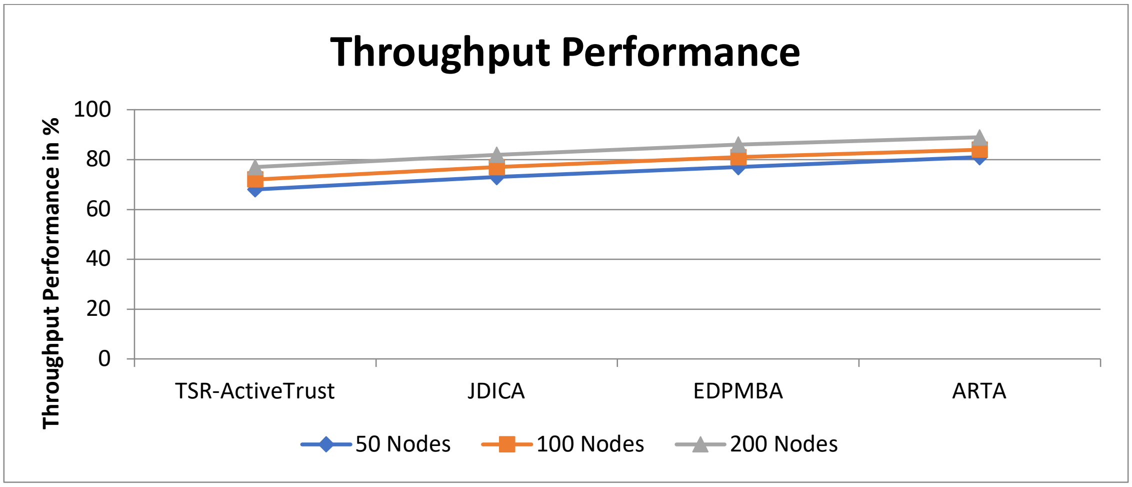

Figure 4: Comparison on throughput performance

The performance introduced in throughput factor by different methods are measured and presented in Figure 4. It has been measured by varying the number of nodes in the simulation as 50 nodes, 100 nodes and 200 nodes. The proposed ARTA scheme has achieved throughput performance than the other approaches.

Packet Delivery Ratio %			
Method	50 Nodes	100 Nodes	200 Nodes
TSR-ActiveTrust	62	66	71
JDICA	65	68	72
EDPMBA	68	73	77
ARTA	73	79	87

Table 5 Packet Delivery Ratio

The packet delivery ratio produced by different methods at the presence of varying node is measured and presented in Table5. The proposed ARTA algorithm has produced higher packet delivery ratio than others.

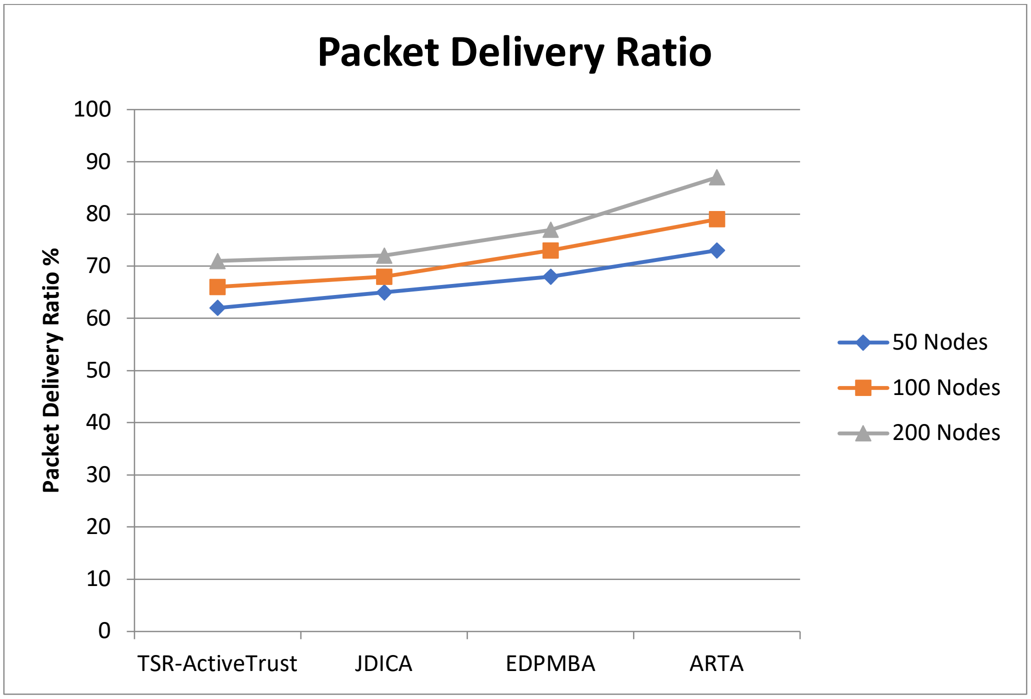

Figure 5: Analysis on packet delivery ratio of STABD vs No of Nodes

The ratio in packet delivery introduced by different approaches are measured and presented in Figure 5. In each test case, the proposed ARTA algorithm produced higher delivery ratio in all the test cases compare to other approaches.

Packet Drop Ratio %			
Method	50 Nodes	100 Nodes	200 Nodes
TSR-ActiveTrust	38	34	29
JDICA	35	32	28
EDPMBA	32	27	23
ARTA	27	21	14

Table 6 Packet Drop Ratio of STABD vs No of Nodes

The packet drop ratio produced by various methods at the presence of varying nodes are measured and presented in Table 6. The proposed ARTA approach has produced less packet drop in all the cases compare to other schemes.

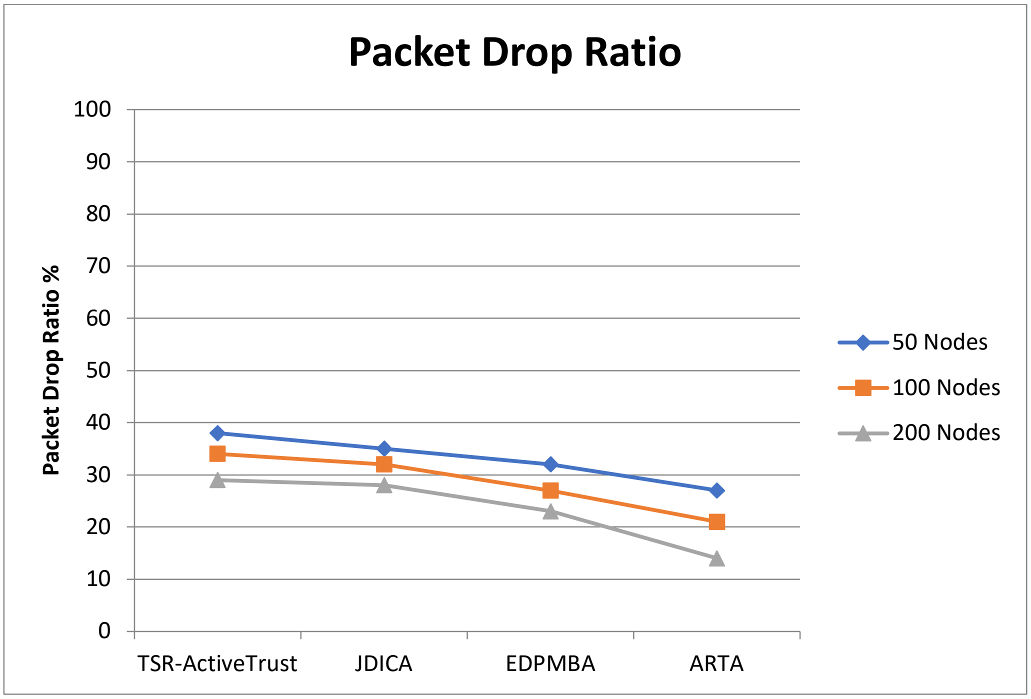

Figure 6: Analysis on packet drop ratio

The ratio of packet being dropped by various approaches at different simulation conditions are measured and presented in figure 6. In each test case, the proposed ARTA algorithm has produced less packet drop than other approaches.

5. Conclusion:

This paper presented a novel adaptive Regional Transmission Approximation Based Black hole Attack Detection for WSN. The method performs route discovery and analyze the regions of network for the presence of malicious nodes. Further, a region has been selected based on the region trust measure (RTM) being measured. The nodes of the region are analyzed with neighbor analysis to compute node trust, based on the node trust, the method selects an optimal route to perform data transmission. The proposed method improves the performance in black hole attack detection and improves the throughput performance.

References:

1. Baviskar B.R, Patil V.N, "Black hole attacks mitigation and prevention in wireless sensor network" International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1 ,Issue 4, pp.167- 169,May 2014.

2. Wang Chun-Hsin and Li Yang-Tang, “Active Black Holes Detection in Ad-Hoc Wireless Networks”, Ubiquitous and Future Networks (ICUFN) 2013 Fifth International Conference on Da Nang, pp.94-99, IEEE, 2013.

3. Mehdi Medadian, Ahmad Mebadi, Elham Shahri, “Combat with Black Hole Attack in AODV Routing Protocol”, Proceedings of the 2009 IEEE 9th Malaysia

International Conference on Communications, 15 -17 December 2009, Kuala Lumpur Malaysia, IEEE 2009.

4. Wazid Mohammad, Katal Avita, Goudar R H,"TBESP Algorithm for Wireless Sensor Network under Blackhole Attack",International conference on Communication and Signal Processing, April 3-5, 2013, India, pp.1086-1091, IEEE 2013.

5. Tiwari Mukesh, Arya Karm Veer, Choudhari Rahul, Kumar Sidharth Choudhary," Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information", Fourth International Conference on Computer Sciences and Convergence Information Technology on Seoul, pp.824-828,IEEE 2009.

6. M. Tokala and R. Nallamekala, "Secured algorithm for routing the military field data using Dynamic Sink: WSN," IEEE (ICICCT), 2018, pp. 471-476.

7. B. Patil and R. Kadam, "A novel approach to secure routing protocols in WSN," IEEE (ICISC), 2018, pp. 1094-1097.

8. F. Mezrag, S. Bitam and A. Mellouk, "Secure Routing in Cluster-Based Wireless Sensor Networks," IEEE (GLOBECOM), 2017, pp. 1-6.

9. C. Deepa and B. Latha, "HHCS: Hybrid hierarchical cluster based secure routing protocol for Wireless Sensor Networks," IEEE (ICICES), 2014, pp. 1-6.

10. R. Shukla, R. Jain and P. D. Vyavahare, "Combating against wormhole attack in trust and energy aware secure routing protocol (TESRP) in wireless sensor network," IEEE (RISE), 2017, pp. 555-561.

11. G. Liu, X. Wang, X. Li, J. Hao and Z. Feng, "ESRQ: An Efficient Secure Routing Method in Wireless Sensor Networks Based on Q-Learning," IEEE (TrustCom/BigDataSE), 2018, pp. 149-155.

12. HIlmi Lazrag, A Game Theoretic Approach for Optimal and Secure Routing in WSN, Springer Link (AECIA), Volume 565, 2016, pp 218-228.

13. M. Kavitha, An efficient city energy management system with secure routing communication using WSN, Springer Link, 2017, PP 1-12.

14. Hanane Kalkha, Hassan Satoria, KhalidSatori, Preventing Black Hole Attack in Wireless Sensor Network Using HMM, Elsevier, Computer Science, vol. 148, pp:552-561,2019.

15. Ganesh R. Pathak, M.S. Godwin Premi, A lightweight Security Framework for Wireless Sensor Networks against the Blackhole Attack, International Journal of Future Generation Communication and Networking, Vol. 13, No. 4, (2020), pp. 129 –135.

16. M. M. Ozcelik, E. Irmak and S. Ozdemir, "A hybrid trust based intrusion detection system for wireless sensor networks," IEEE (ISNCC), 2017, pp. 1-6.

17. Z. Sun, Y. Xu, G. Liang and Z. Zhou, "An Intrusion Detection Model for Wireless Sensor Networks With an Improved V-Detector Algorithm," in IEEE Sensors Journal, volume 18, number 5, pp. 1971-1984, 2018.

18. V. T. Alaparthy and S. D. Morgera, "A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory," in IEEE Access, volume 6, pp. 47364-47373, 2018.

19. Higo Pires, A framework for agent-based intrusion detection in wireless sensor networks, ACM (ICC), 2017.

20. Christiana Ioannou, An Intrusion Detection System for Constrained WSN and IoT Nodes Based on Binary Logistic Regression, ACM (MSWIM), 2018, PP 259-263.

21. Adwan Yasin and Mahmoud Abu Zant, Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique, Wireless Communication and Mobile Computing, Hindawi, vol. 2018, 2018.

22. Ankit Kumar, Vijayakumar Varadarajan, Abhishek Kumar, Pankaj Dadheech, Surendra Singh, Choudhary, V.D. AmbethKumar, B.K.Panigrahi, Kalyana C.Veluvolu, Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm, Micro processor and micro systems, vol 80, 2021.