SECURITY ENHANCEMENTS OVER AODV USING MULTI-HOP ACKNOWLEDGMENT

Aditya Saravanan, Arjun Pant and A. Jeyasekar
Dept. of CSE, SRM Institute of Science and Technology,Chennai, Tamil Nadu

ABSTRACT

In most applications of Mobile Ad-hoc Networking and Wireless Sensor networks (WSNs), security and power consumption is a recurring problem which is very difficult to solve due to unpredictable behaviour, environmental changes and mobility of nodes. TERP is a Trust based Energy Routing Protocol that considers the energy conservation and security aspects of WSNs. It is an improved version of AODV and ensures low power consumption while adding a trust based system to the reactive nature of AODV. It also provides the solutions for the most basic attacks like node selfishness, spoofing, misbehaviour and packet sniffing. But black-hole attack, gray-hole attack, Sybil and wormhole attacks are yet to be addressed in the TERP. This paper provides a solution to detect and prevent the node misbehaviour and gray-hole attack. TERP identifies the node misbehaviour using direct and indirect trust recommendations received from neighbour nodes. The detection rate of misbehaving nodes is less during the initial life of the network. Therefore we propose a method that detects the node misbehaviour during the initial life by using a multi-hop acknowledgement system. The simulation results show that the proposed method performs well in detecting the gray-hole and node misbehaviour.

KEYWORDS

AoDV, TERP, NACK, Multihop Acknowledgement, Blackhole Attack, Grayhole Attack

1.INTRODUCTION

In recent years, Wireless Sensor networks (WSNs) and Mobile Ad-hoc networks (MANETs) have gained relevance in various aspects of our lives. WSNs are expected to operate independently without human supervision which makes the network vulnerable to a variety of attacks such as black hole, selective forwarding, Sybil attack, HELLO flood attack, wormhole, and Identity replication attack [7]. In addition to this, most WSNs are battery operated networks hence power consumption is to be considered while developing a new protocol. The traditional security measures and key management algorithms require high computational power and memory which are to be restricted in the WSNs [8-11]. Low routing overhead and computational tasks are the primary design requirements of WSN routing algorithms to reduce power consumption.

There are many energy aware routing protocols [12-16] and security aware routing protocols [17-21] used in the WSNs. Energy aware routing protocols maintain low energy states in periods of inactivity but they do not appropriately tackle the issue of node misbehaviour while maintaining a low routing overhead [14][16] The security aware routing protocols need a low complexity algorithm for encryption and key management in order to maintain the energy conservation.

TERP is a derivative of AODV routing protocol that uses a trust based routing algorithm and it attempts to reduce power consumption as well as integrate the energy awareness feature with the route discovery process [1]. TERP has mechanisms to create end-to-end routes while keeping the energy levels of the intermediate nodes in mind. It estimates the trust level of a neighbouring node by determining the ratio correctly forwarded packets to the number of incoming packets. The trust estimation starts after the inception of the network by observing the behaviour of the nodes within the network. It takes some time for collecting the sufficient amount of data transaction from the

DOI: 10.5121/ijwmn.2020.12201

nodes in the networks to estimate the trust level of neighbour nodes. This vulnerable time provides a window of opportunity for the misbehaving nodes to steal the data.

Therefore, in this paper, the vulnerable time of TERP protocol is taken into account and mitigates the misbehaving node by using multi-hop acknowledgement method. This paper is organized as follows: Section II covers the related works, specifications of TERP and its weaknesses. Section III covers our proposed solution to the vulnerabilities of TERP. Finally we conclude the paper in Section IV.

2.RELATED WORKS

In this section, the energy-aware and trust based routing algorithm are discussed. First the TERP protocol and its trust estimation are presented and the other routing protocols are discussed next. Since the TERP [1] is developed for WSNs, it listens to the transmissions of all of its next hop neighbours with the assumption that each node has a similar range of resources such as power and computational capability. TERP does not allow nodes to be added or removed after deployment of the network. All nodes in the network monitor their neighbouring nodes to establish their trust values. The nodes are only concerned with their next hop neighbours in a transmission. The trust value of a node is generated as a result of Direct and indirect trust. Trust values range from 0 to 1 where 1 represents a perfectly trusted node and 0 represents a malicious node. The total trust of a node is represented as:

$$T_{i,j}\,(t) = w_1 DT_{i,j}\,(t) + w_2 \frac{IT^{k}_{i,j}(t)}{N_j}$$

Ti,j (t) denotes the degree of trust that a node i has for node j at time t. DTi,j (t) denotes the degree of direct trust that a node i has for node j at time t, based on the node i’s observation of packet forwarding behaviour for node j. ITki,j(t) represents the average degree of indirect trust node i has gained using recommendations from its neighbours (k) for node j at time t. Nj represents a set consisting of neighbours for node j [1]. The weight factors w1 and w2 represent the weightages assigned to direct trust and indirect trust.

TERP is a reactive protocol and does route discovery before every transmission. It adds the Energy Awareness factor into the route setup phase by not allowing any untrustworthy or low energy nodes in the route. When the sender node transmits the RREQ packet, the packet is only sent to trusted nodes which have energy levels above the minimum threshold. This forms a route consisting of nodes which are trusted and have a power level above the minimum threshold. If any node in the route is no longer trusted or its power level falls below the minimum threshold, then a route maintenance procedure creates an alternate route excluding the node that needs to be removed. The trust estimation phase of TERP utilizes promiscuous listening in order for the nodes to listen to the forwarded packets of its next hop neighbours to check if they are correctly forwarding the packet[1]. The nodes in TERP need to listen to a packet twice during the transmission of the packet through the network, once when they receive the packet, and once to verify the authenticity of the packet forwarded by its next hop neighbour. The most power consuming component of any node is the RF transmitter and receiver, and using it twice for every packet transmission makes it somewhat inefficient. Wormhole attacks are not able to be detected by TERP since it assumes that all misbehaving nodes do not collaborate with other misbehaving nodes and the wormhole attack consists of two nodes cooperating to tunnel packets and reduce network availability. It also cannot counter Sybil attacks since TERP is not able to solve the issue of nodes assuming false identities. TERP achieves better results for latency, throughput and power efficiency and also has better security than AODV [1], TARF [22] and TSRF [23] but its performance in heterogeneous network is less [1][22]. This is because TERP assumes that each node has similar capabilities in terms of energy, computing power and memory. TERP uses battery threshold in terms of percentage hence in heterogeneous networks where battery capacities vary greatly, the TERP is unable to perform at its best in the heterogeneous network. As of now, TERP is also unable to counter node selfishness or Grayhole attacks but has managed to somewhat mitigate node misbehaviour [1]. TERP has an issue of misidentifying faulty nodes as misbehaving nodes but it is limited to certain rare test cases where nodes get congested immediately after the deployment of the network [1]

In [3], Jian Ming Chang et al uses a bait based detection strategy where a node sends a RREQ packet across the network for a node directly adjacent to it, any node that sends a false RREP is detected since the destination node is adjacent. The issue with this approach is that it can black hole attackers but grayholes do not violate node based trust in the route discovery phase. [4] uses a methodology similar to TERP in the fact that it also uses a trust-based route evaluation but it uses reputation by creating a separate phase for reputation evaluation where all nodes calculate the reputation of their neighbouring nodes. This procedure is carried as a short term measure of reputation and is not used for the entirety of the network lifetime. The reputations of the neighbouring nodes are then propagated across the network. The nodes then integrate the shared reputation values with their own reputation estimation to create reputation values for the nodes in the network. This is very similar to TERP, the only significant differences being the fact that malicious nodes which start misbehaving later are caught relatively easily since reputation is not cumulative over a long time, while having the disadvantage of increased computation time and routing overhead due to repetitive reputation estimation. In [5], Qiang Liu et al uses a checkpoint in the route generated randomly and uses it to verify whether the message reaches the checkpoint to try and isolate misbehaving nodes. The checkpoint acts to constrict the area of suspicion by sending the source an ACK message and forwarding the packet to its intended destination. A two-hop acknowledgement and node evaluation algorithm are used in [6] to detect malicious nodes downstream along the route in an incremental fashion.

3.PROPOSED SYSTEM

The TERP protocol despite its weaknesses utilises a simple routing function and manages to elegantly add energy awareness and trust based forwarding node selection to the route setup phase. The trust based routing protocol is unable to mitigate some attacks such as grayhole attack, or selective dropping and node misbehaviour attack. Hence in this paper, we propose a method for detecting grayhole attacks using the multi-hop acknowledgement scheme. When a packet loss is very high, then the proposed method tries to isolate the misbehaving nodes from the routing of packets using multihop acknowledgement scheme and Negative Acknowledgement.

Fig 1 presents the concepts of proposed multihop acknowledgement scheme that is incorporated along with AODV in order to isolate the misbehaving nodes in WSN.

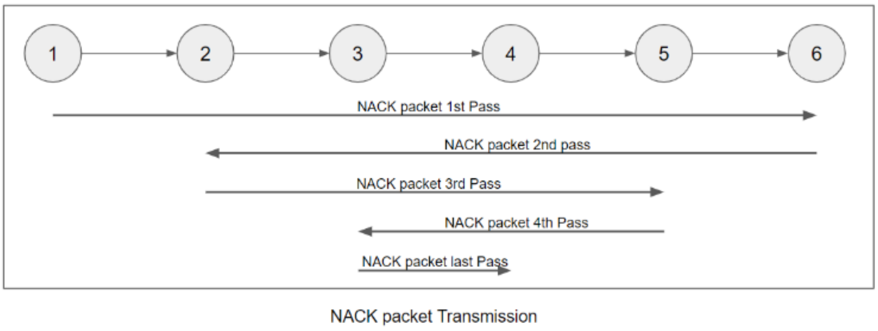


Fig 1. The concept of proposed multihop acknowledgement scheme

In the proposed scheme, a new packet type called NACK is created which is similar to the IP packet header. The NACK packet is treated as a data packet and not a control packet, and hence malicious nodes will attempt to drop the packet. The NACK packet is only sent if the packet loss ratio exceeds a certain threshold in trust based protocols. In our implementation in the AODV routing protocol, we have triggered the packet randomly. Once the NACK packet is sent, the sender waits for ACK from the next two nodes in the route. The sender and every intermediate node should receive an ACK from the next two successive hop nodes in the route. This method is similar to promiscuous listening, but is more concrete as it requires an acknowledgement from the next-to-next hop to confirm that the next hop has forwarded the packet. If an ACK is not received from some of the nodes in the route, then the node that sends the last acknowledgement and the node which has not sent an acknowledgement are blacklisted. We are not considering the possibility of faulty nodes since trust based protocols such as TERP[1] have already made considerations for the issue. The packet header stores the source, destination and the first hop from the source for forwarding for the next pass. We use multiple passes since grayhole attacks also attack selective IP addresses and we have attempted make sure that the packet transmission happens in such a manner that every node in the route will forward packets intended to every other node in the route, i.e during the method after every pass, the first hop from the source will become the next destination and in this manner every node will be a destination allowing any selective grayhole attacker to drop the packet.

The proposed method comprises four algorithms: 1) NACK packet and diagnostic initialization 2) Handling of NACK packet ,3) Detection of misbehaving nodes and isolation and 4) NACK acknowledgement processing.

When the proposed method encounters high packet loss, then the source sends a NACK packet to the destination as given in Algorithm 1. The packet records the route nodes as it reaches the destination node.

Algorithm 1: NACK packet and diagnostic initialization.

```
Initiate NACK packet from transmission source
Set Dstn same as the previous packet destination
Lookup next hop and record it in the packet header..
Send the packet
Set ACK timer for next two nodes
If ACK.is received from each node
        cancel the corresponding timers
```

If the packet does not reach the destination, there is a possibility of grayhole attacker in the path to destination. So that the packets intended for the destination node is dropped by the grayhole node. Hence the proposed method tries to send a packet from the first hop to the destination to shorten the area of detecting the misbehaving nodes as shown in Algorithm 2. As the packet is forwarded, each node sets a timer for an acknowledgement for the next two hops as shown in Algorithm 1. It also sends an Acknowledgement packet to its preceding node which is also forwarded to the node before it.

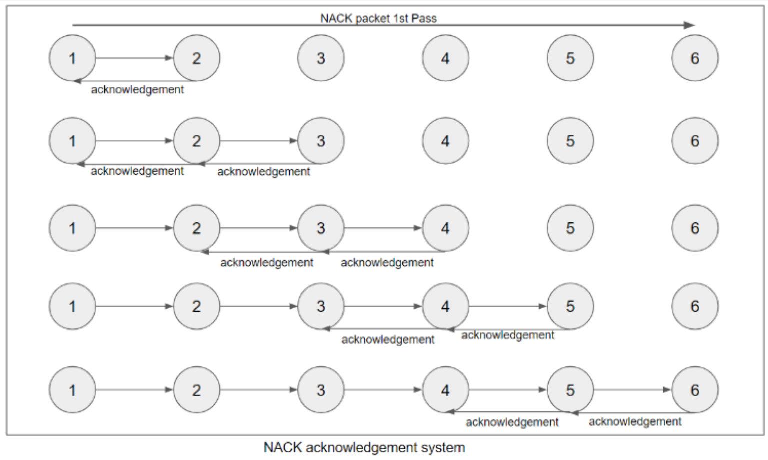


Fig 2. The acknowledgement scheme for NACK packets

Once the destination is reached, the packet is forwarded to the first hop recorded in the packet hence excluding the first node from the area of suspicion. This reduces the area of detecting the misbehaving nodes by excluding the source node from the area of suspicion as well as confirms that the grayhole is not dropping packets intended for the destination node n_d. If the packet reaches the destination (first node), we can assume that the destination node can also be trusted and that the grayhole isn't dropping packets intended towards the first hope node n_1. The node n_1 then forwards the packet to n_{d-1} node (first hop in the recorded route as shown in Algorithm 2.

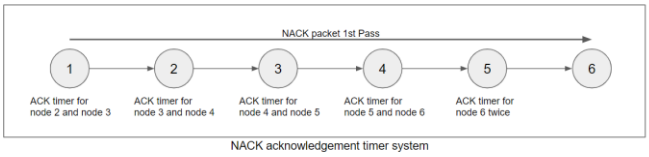
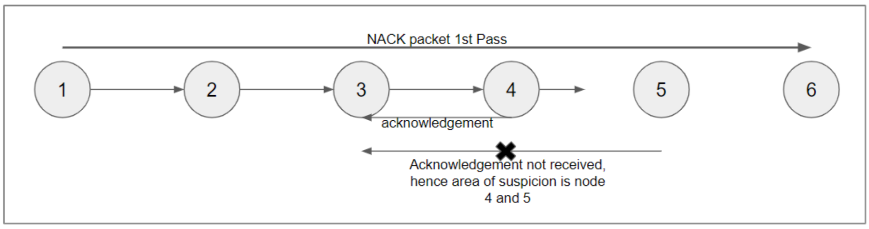

NACK packet 1st Pass
1
2
3
4
5
6
ACK timer for node 2 and node 3
ACK timer for node 3 and node 4
ACK timer for node 4 and node 5
ACK timer for node 5 and node 6
ACK timer for node 6 twice
NACK acknowledgement timer system

Fig 3. The acknowledgement timer setup for each node in a single pass

Algorithm 2: NACK packet handling

```
1: If DSTN != Node Address
        forward packet to the next hop using Algorithm 1.
        Set timer for acknowledgement
        Send ACK to previous hop
2: If DSTN = Node Address
        Start NACK initialization procedure.
        Send ACK to the previous hop neighbor .
        Set Destination as the first hop from the current NACK packet's header..
End procedure.
```

The proposed method keeps on eliminating nodes by labelling them as trustworthy one by one to isolate an area of suspicion. Once the proposed method has found a malicious node or has labeled a node as unidirectional it re-initiates route discovery and sends hello packets as shown in Algorithm 3 to update the routing tables of all nodes regarding the newly blacklisted node. If the packets are still dropped, then the proposed method proceeds to execute the method in the area of suspicion to find more malicious nodes.

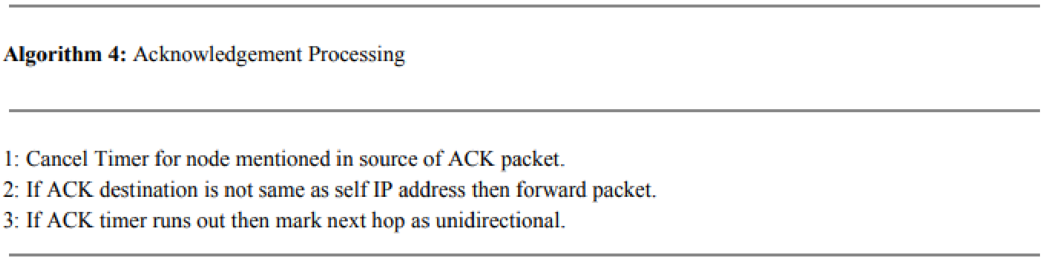

NACK packet 1st Pass
1
2
3
4
5
6
acknowledgement
Acknowledgement not received, hence area of suspicion is node 4 and 5

NACK Malicious node detection

Fig 4.Malicious node detection in proposed scheme

Once the procedure is complete, it re-initiates route discovery and hello packets to update the routes and check if any other nodes have been blacklisted by other nodes participating in the method. This method will execute multiple times since blackhole attackers will exist on different routes and this algorithm detects attackers within the route. The method has been set to not activate for a certain period of time after completion to avoid excessive power consumption caused as a result of the method. This is achieved using a timer on all the nodes which participate in the procedure

1: If Area of Suspicion is set
then procedure continues on the nodes alongside packet transmission till a misbehaving node is detected or procedure completes
2: If a malicious node is detected, the procedure stops since the NACK hasn't been forwarded and the node is marked as unidirectional by its preceding node.
3: If a node has been marked unidirectional, the preceding node initiates a Hello packet and a RREQ to its neighbours so that the routing tables can be updated with the new malicious node blacklisted.
4: If the procedure is complete, the final node to receive the NACK packet initiates a Hello packet and a RREQ to update all routing tables



Algorithm 4: Acknowledgement Processing

```
Cancel Timer for node mentioned in source of ACK packet.
If ACK destination is not same as self IP address then forward packet.
If ACK timer runs out then mark next hop as unidirectional.
```

The algorithm 4 used for Acknowledgement processing is not responsible for marking the node as unidirectional, but a timer initiates a callback to the function set on the timer once it expires and is actually part of Algorithm 2 where the timer is set for the next and next-to-next hop neighbours.

4.PERFORMANCE ANALYSIS

The proposed method is evaluated using NS-3.29 with 1000 nodes in 800 x 1200m grid and simulating 20 packet flows with a randomized number of blackhoe and grayhole nodes for a total time of 30 seconds. The nodes are stationary for some time as well as mobile for randomized periods of time. The total number of malicious nodes has been varied from 1 to 10 for the simulation. We have measured throughput, number of packets dropped and the number of nodes detected as the parameters for measurement

Table 1. NS – 3.29 Simulation environments

Simulator	NS-3 Version 3.29
Simulation area	800 x 1200 m^2
Number of Wired Node	0
Number of Base Station	0
Number of wireless Node	100
Propagation model	Friis Propagation Loss Model
Routing protocol	AODV
Simulation time	30 s
Bit Rate	CBR(Constant Bit Rate)

The proposed method provides better performance and is able to detect almost all the blackhole nodes and several grayhole nodes. The number of misbehaving nodes detected at the end of the simulation with respect to the total number of misbehaving nodes introduced in the simulation. The Grayhole nodes are not selective grayholes and use a randomized function to drop packets. The performance of the proposed method is evaluated by introducing more misbehaving nodes in the simulation. But beyond a value, the proposed diagnostic method is invoked too many times which leads to reducing efficiency of the network.

The success rate of detecting the blackhole attack is high for a small WSN. But the performance of the proposed method is reduced as the number of blackhole nodes increases. This is because the method cannot be repeatedly invoked in a short time period. We have used a function to limit the number of times the procedure can be called within a period of time using a timer. But this also limits the detection capabilities in case of a large number of malicious nodes.

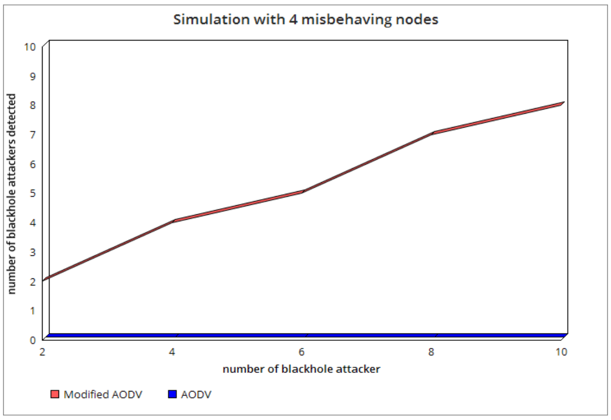


Fig 5. Blackhole attacker detection rate

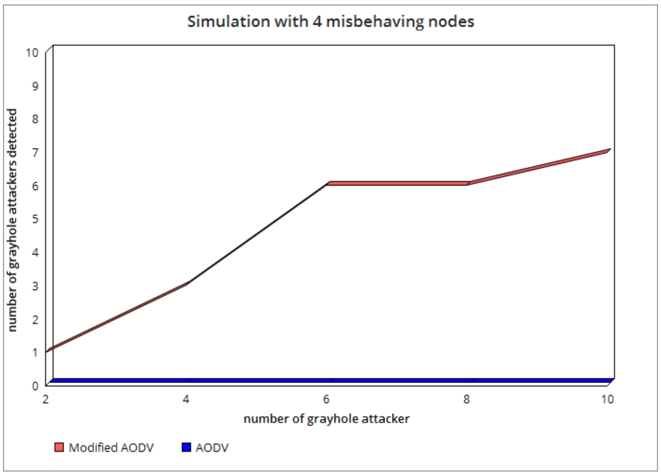


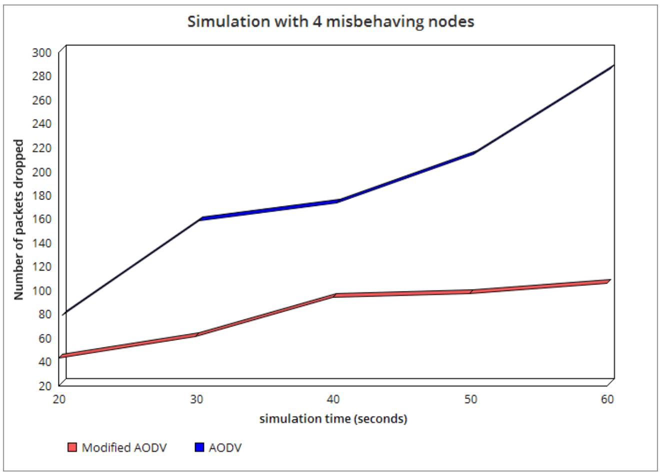
Fig 6. Grayhole attacker detection rate

I. Malicious node Detection

We have tested the method with the intention of it being an add-on to existing trust schemes where malicious nodes are adapted to the trust system as well. The method is able to detect Blackhole and Grayhole attackers and is able to do so with restrictions on how many times it can be called. However, its efficacy is reduced with a higher number of attackers.

II. Throughput

The Throughput was affected as the number of malicious nodes increased, though not as adversely as in the case of AODV since the methodology consumes network bandwidth, but is not as detrimental as the effect caused by malicious nodes. TERP has better performance since it is a hybrid protocol unlike AODV upon which the method is built, but the method will have a lesser impact on throughput if it worked in tandem with any trust based protocols.



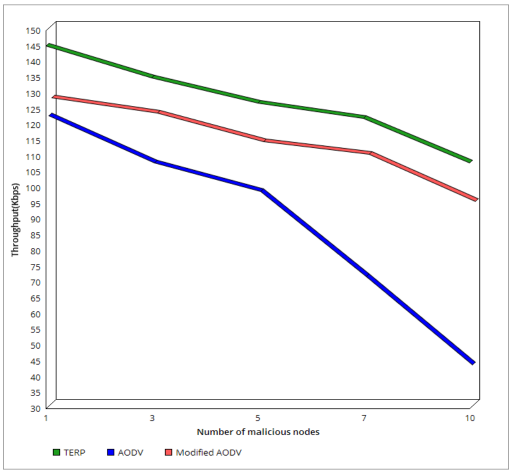
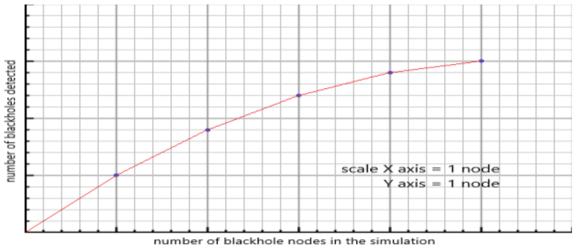
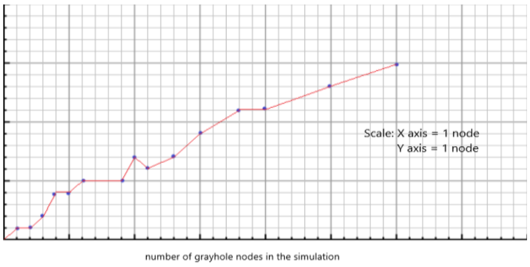


Fig 7. Number of packets dropped

Fig 8. Throughput vs Malicious nodes

As for Grayhole nodes, the results weren't as conclusive and malicious nodes were not always detected. Each test was run 5 times to get a mean of the number of detected nodes and the results varied due to the random nature of grayhole nodes. However, selective grayhole nodes were easily detected and added to the blacklist. This was not the case for probabilistic grayhole nodes which attack based on a randomized function in our simulation. The ideal case scenario was for 4 grayhole nodes where all of them were detected 4 out of 5 times





CONCLUSION

The proposed method provides the solution for the issues with TERP routing protocol. The proposed algorithm is able to avoid the excessive power consumption needed to do a comprehensive search for detecting the misbehaving nodes in the route. The proposed algorithm detects and isolates the blackhole and grayhole attackers in WSN in a better way than TERP. The method is less effective against multiple attackers in close proximity to each other as the algorithm will activate too many times which is detrimental to overall throughput since the algorithm is time consuming and cannot run for too long or multiple times without reducing efficiency drastically. The performance of the proposed algorithm in detecting the grayhole nodes is to be improved further in order to provide 100% detection

REFERENCES

[1] TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb, and Abdul Waheed Khan 2015

[2] Intrusion Detection and Prevention Based on State Context and Hierarchical Trust in Wireless Sensor Networks R Maidhili ; GM Karthik 2018

[3] Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, Member, IEEE 2015

[4] Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks Ju Ren, Student Member, IEEE, Yaoxue Zhang, Kuan Zhang, Student Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE 2016

[5] A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation Cong Pu, Student Member, IEEE, and Sunho Lim, Member, IEEE 2018

[6] FADE: Forwarding Assessment Based Detection of Collaborative Grey Hole Attacks in WMNs Qiang Liu, Jianping Yin, Victor C. M. Leung, Fellow, IEEE, and Zhiping Cai, Member, IEEE 2013

[7] H. Modares, R. Salleh and A. Moravejosharieh, "Overview of Security Issues in Wireless Sensor Networks," 2011 Third International Conference on Computational Intelligence, Modelling & Simulation, Langkawi, 2011, pp. 308-311.

[8] J. Yao, "A Security Architecture for Wireless Sensor Networks Based-On Public Key Cryptography," 2009 5th International Conference on Wireless Communications, Networking and Mobile Computing, Beijing, 2009, pp. 1-3.

[9] P. G. Shah, X. Huang and D. Sharma, "Analytical Study of Implementation Issues of Elliptical Curve Cryptography for Wireless Sensor networks," 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, Perth, WA, 2010, pp. 589-592.

[10] K. Bicakci, H. Gultekin and B. Tavli, "The impact of one-time energy costs on network lifetime in wireless sensor networks," in IEEE Communications Letters, vol. 13, no. 12, pp. 905-907, December 2009.

[11] K. Ravi, R. Khanai and K. Praveen, "Survey on pairing based cryptography for wireless sensor networks," 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, 2016, pp. 1-4.

[12] J. Vazifehdan, R. V. Prasad and I. Niemegeers, "Energy-Efficient Reliable Routing Considering Residual Energy in Wireless Ad Hoc Networks," in IEEE Transactions on Mobile Computing, vol. 13, no. 2, pp. 434-447, Feb. 2014.

[13] T. Zhang, J. Cao, Y. Chen, L. Cuthbert and M. Elkashlan, "A Small World Network Model for Energy Efficient Wireless Networks," in IEEE Communications Letters, vol. 17, no. 10, pp. 1928-1931, October 2013.

[14] Y. Zhu, M. Huang, S. Chen and Y. Wang, "Energy-Efficient Topology Control in Cooperative Ad Hoc Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1480-1491, Aug. 2012.

[15] A. Taha, R. Alsaqour, M. Uddin, M. Abdelhaq and T. Saba, "Energy Efficient Multipath Routing Protocol for Mobile Ad-Hoc Network Using the Fitness Function," in IEEE Access, vol. 5, pp. 10369-10381, 2017.

[16] Deying Li, Xiaohua Jia and Hai Liu, "Energy efficient broadcast routing in static ad hoc wireless networks," in IEEE Transactions on Mobile Computing, vol. 3, no. 2, pp. 144-151, April-June 2004.

[17] P. Papadimitratos and Z. J. Haas, "Secure data communication in mobile ad hoc networks," in IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 343-356, Feb. 2006.

[18] M. Ramkumar and N. Memon, "An efficient key predistribution scheme for ad hoc network security," in IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 611-621, March 2005.

[19] R. Lacuesta, J. Lloret, M. Garcia and L. Peñalver, "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation," in IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 4, pp. 629-641, April 2013.

[20] G. Acs, L. Buttyan and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," in IEEE Transactions on Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[21] A. M. Shabut, K. P. Dahal, S. K. Bista and I. U. Awan, "Recommendation Based Trust Model with an Effective Defence Scheme for MANETs," in IEEE Transactions on Mobile Computing, vol. 14, no. 10, pp. 2101-2115, 1 Oct. 2015.

[22] G.Zhan, W. Shi and J. Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs," in IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, pp. 184-197, March-April 2012.

[23] TSRF: A Trust-Aware Secure Routing Framework in Wireless Sensor Networks International Journal of Distributed Sensor Networks. 2014;10