Advances in Technology Innovation, vol. 2, no. 4, 2017, pp. 113 - 118

Securing Ad Hoc Wireless Sensor Networks under Byzantine Attacks by Implementing Non-Cryptographic Methods

Shabir-Sofi[1,*], Roohie-Naaz[2]

[1]Department of Information Technology, National Institute of Technology Srinagar, India.

[2]Department of Computer Sciences & Engineering, National Institute of Technology Srinagar, India.

Received 10 December 2016; received in revised form 16 February 2016; accepted 08 March 2017

Abstract

Ad Hoc wireless sensor network (WSN) is a collection of nodes that do not need to rely on predefined infrastructure to keep the network connected. The level of security and performance are always somehow related to each other, therefore due to limited resources in WSN, cryptographic methods for securing the network against attacks is not feasible. Byzantine attacks disrupt the communication between nodes in the network without regard to its own resource consumption. This paper discusses the performance of cluster based WSN comparing LEACH with Advanced node based clusters under byzantine attacks. This paper also proposes an algorithm for detection and isolation of the compromised nodes to mitigate the attacks by non-cryptographic means. The throughput increases after using the algorithm for isolation of the malicious nodes, 33% in case of Gray Hole attack and 62% in case of Black Hole attack.

Keywords: byzantine attacks, cluster based wireless sensor network, advanced node, gray hole, black hole, non-cryptographic

1. Introduction

Wireless Sensor Network (WSN) is a type of Ad Hoc networks having large number of the nodes. The nodes of the WSN may be static or mobile as in case of other Ad Hoc networks. The wireless sensor networks pose unique challenges as the sensor nodes are limited in their energy, computation and communication capabilities. Also, the sensor nodes are deployed in inaccessible areas to monitor physical environment. The sensor nodes may be thousands in number to collectively monitor an area. As a result, the existing security mechanisms are inadequate [1]. Since all the nodes in an area usually detect common phenomenon, this leads to high data redundancy. To save energy and prolong network lifetime, an efficient way is to aggregate the raw data before they are transmitted to the base station as the sensor nodes are resource limited and energy constrained. Data aggregation is an essential paradigm to eliminate data redundancy and reduce energy consumption [2-3]. The level of security and performance are somewhat related to each other. A WSN application usually requires different functionalities, sensing, storing data, and data communication. Sensing usually require a large number of nodes to ensure coverage and few resources on each node. In contrast, data transmission and data storage require more system resources.

Data aggregation is an essential paradigm to eliminate data redundancy and reduce energy consumption. The data ag-gregation is used in WSN to reduce the communication overhead and prolong the network lifetime. However, an adversary may compromise some nodes and use them to forge false values as the aggregation result. For securing data aggregation, we need to detect the malicious nodes which add to overhead due to encryption, decryption and sharing of keys.

Tiered network design with functional partition prolongs network lifetime instead of homogeneous network. Clustering in WSN, where groups of sensor nodes select their cluster head depending on the energy level [4, 14] or in some applications the cluster can be fixed at the time of deployment [5]. Whether the cluster head is pre-decided or selected by the individual nodes of the group the network will be ad hoc in either case.

For many applications, the sensed readings are sensitive and thus demand for data security, confidentiality, integrity and freshness. However, the tight resource constraints of wireless sensors restrict the adoption of traditional computation intensive algorithms. A compromised storage agent may reveal its saved readings, drop important readings, compose forged data readings and reply old data readings. Without carefully designed security enhancements, the above attacks can leave the network useless in a hostile environment. There is no secure boundary in Ad Hoc networks, making the network susceptible to attacks, since Ad Hoc networks suffer from all-weather attacks which may come from any node in the network. There are other link attacks also which can jeopardize the Ad Hoc network [6]. These include eavesdropping, active interfering and leakage of secret information, data tampering, message reply, message contamination and denial of service attacks.

The attacks where aim is to gain control over WSN nodes by some unrighteous means and then using these compromised nodes to execute further malicious actions. The threats of such attacks are usually from inside the network and these threats are more dangerous than the threats from outside the network. These attacks are difficult to detect as they come from compromised nodes, which behave well before they are compromised. A good example of this type of threats comes from the potential Byzantine failures encountered in the routing protocol for the ad hoc networks. In a Byzantine failure, a set of nodes are compromised in such a way that the incorrect and malicious behaviour cannot be directly detected because of the cooperation among these compromised nodes when

*Corresponding author. Email: address:shabir@nitsri.net
Tel.: +91-9419009971

they perform malicious behaviours. The compromised nodes may seemingly behave well; however they may actually make use of the flaws and inconsistencies in the routing protocol to undetectable destroy the routing fabric of the network, generate and advertise new routing information that contain non-existent link, provide fake link state information, or even flood other nodes with routing traffic.

It is common in ad hoc networks that benign failures such as path breakages, transmission impairments and packet dropping, happen frequently. Hence malicious failures will be more difficult to detect especially when adversaries change their attack pattern and their attack target in different periods of time.

1.1. Attacks in Ad Hoc Networks

There are numerous types of attacks in ad hoc network, which may be classified into two types, external attacks and internal attacks. External attack, in which the attacker aims to cause congestion propagate fake routing information or disturb nodes from providing services. In internal attack, in which the adversary wants to gain access to the network activities, either by some impersonation or by directly compromising a current node and using it as basis to conduct its malicious behaviors [7]. In an internal attack adversary can capture some nodes in the network and make them look like benign nodes, these nodes join the network as the normal nodes and begin to conduct the malicious behaviors like propagating fake routing information and begin inappropriate priority to access some confidential information [22]. The internal attacks are sometimes more severe threat to the security than external attacks as they are difficult to detect at an early stage.

1.2. Routing Attacks

Routing attacks are classified into two categories: attacks on routing protocols and attacks on packet forwarding. The main influences brought by the attacks on routing include network partition, route loop, resource deprivation and route hijack. Because of the mobility and constantly changing topology of the mobile ad hoc networks, it is very difficult to validate all the route messages as a result, impersonating another node to spoof route message, advertising false route metric to misrepresent topology, flooding route discovery, modifying route reply message, generating bogus route error to disrupt a working route, suppressing route error to mislead others may occur. In packet forwarding/delivery selfishness and denial-of-Service are the two main strategies applied for the attack.

1.3. Byzantine Attacks

When a network device suffers a byzantine fault it is assumed to be controlled by an adversary who uses the device to disrupt the network [16]. The goal of the Byzantine node is to disrupt the communication of other nodes in the network, without regard to its own resource consumption. These cause Byzantine failures which include the omission failures and commission failures. As for instance in omission failures if a node fail to receive a request or fail to send a response and in commission failures if a node process a request incorrectly or sending an incorrect or inconsistent response to a request. In Ad Hoc networks, the Byzantine attacks are as: Black Hole attack, Gray Hole attack, Flood Rushing attack and Wormhole attack. Wireless sensor networks are favorite targets of Byzantine attacks because of their limited dynamic topology etc. [21].

1.4. Black Hole Attack

It is a basic Byzantine attack [9] where adversary stops forwarding data packets, but still participates in the routing protocol correctly. As a result, whenever the adversarial node is selected as part of a path by the routing protocol, it prevents communication on that path. Most routing protocols are disrupted by Black Hole attacks because they render the normal methods of route maintenance useless.

1.5. Gray Hole Attack

It is a special case of black hole attack where an attacker could create a grey hole, in which it is selectively drops some packets but not others, for example forwarding some packets but not data packets[10].

1.6. Wormhole Attack

If more than one node is compromised, it is reasonable to assume that these nodes interact in order to gain an additional advantage. This allows the adversary to perform a more effective attack. One such attack is Byzantine Wormhole where two adversaries tunnel packets between each other in order to create a shortcut (or Wormhole) in the network. The adversaries can send a route request and discover a route across the Ad Hoc network, then tunnel packets through the non-adversarial nodes to execute the attack. The adversaries can use the low cost appearance of the wormhole links in order to increase the probability of being elected as part of the route and then attempt to disrupt the network by dropping all of the data packets. The Wormhole attack is strong attack which can be performed even if only two nodes are compromised.

1.7. Flood Rushing Attack

A flood rushing attack [12] exploits the flood duplicate suppression technique used by many routing protocols. This attack takes place during the propagation of legitimate flood and can be seen as a “race” between the legitimate flood and the adversarial variant of it. If an adversary successfully reaches some of its neighbors with its own version of the flood packet before they receive a version through a legitimate route, then those nodes will ignore the legitimate version and will propagate the adversarial version. This may result in the continual ability to establish an adversarial-free route, even when authentication techniques are used.

When a node wants to send a packet, it will send route request packet and if it receives a route reply first from a normal behaving node, then everything will work fine. However, if it gets reply from an attacker node, all the packets will not reach the destination or there may be selective dropping. In both the cases the delivery ratio will decrease. Therefore, identification of such nodes is the first step in preventing their participation in the data transfer. Also, a route reply from an attacker node can

reach the source node earlier than a normal node if it is near to the source node. Since each node in a homogeneous WSN, acts as router, the data transmission from source to the gateway occurs via different sensor nodes, while in case of heterogeneous network the individual nodes may or may not participate in the routing process.

The homogenous WSN can be treated as a special case of ad hoc networks where the number of nodes is very large as compared to the ad hoc network. The detection and isolation of an attacker node is difficult. Also, the packet delivery ratio will be lesser. In heterogeneous WSN the nodes are grouped in clusters and each node in the cluster transmits its data via the cluster head (CH) [4, 14]. Since the nodes in cluster are fewer as compared to the nodes in a homogeneous WSN the chances of detection and isolation of the attacker node are more.

Karlof et al. [13] proposed selective forwarding attack for the first time in wireless sensor networks and suggested that multipath forwarding to counter the attack. But, the algorithm fails to suggest a method to isolate the attacking node. Marti et al. [11] proposed a technique called Watchdog, in which a node continuously monitors the neighboring nodes to which the packet is sent and to check whether the packet is forwarded or not. But the algorithm fails to detect the attacker in the presence of selective forwarding attack.

2. Comparison LEACH and advanced node

In Fig. 1, LEACH vs. Advanced node based network the probability of sustaining the black hole or gray hole attack is more in the advanced node based network as compared to LEACH based network. Also the life cycle of the nodes in Advanced node based network is more than the LEACH based network. During the cluster head selection process and after becoming cluster head the node consume almost n+1 times the energy consumed by an individual sensor node. Since data aggregation as well as the routing of the other information from and to the nodes is carried through the cluster head, in addition to its own sensing and data transmission which leads to quicker energy depletion.

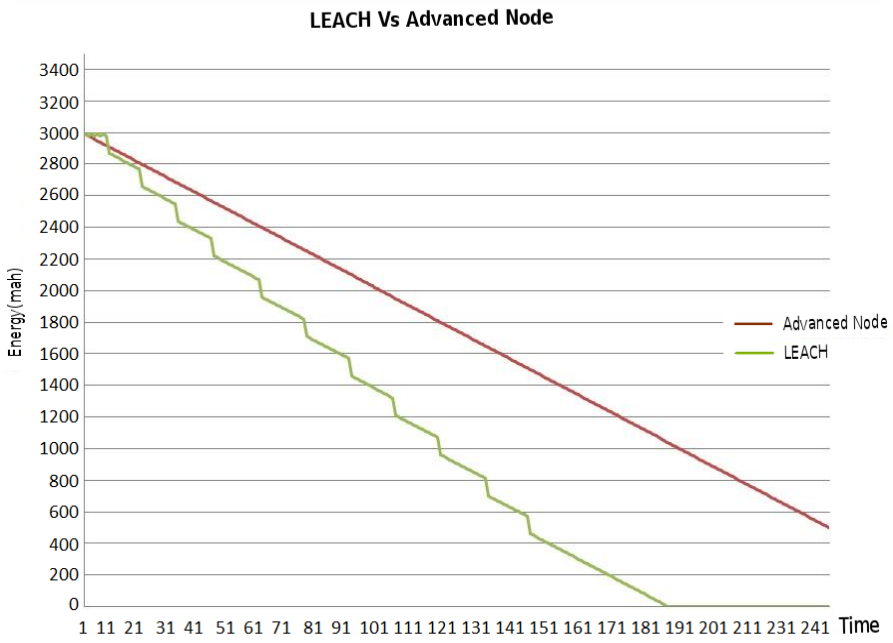

Fig. 1 Advanced node based protocol vs. LEACH protocol. (Energy in mah and time in days with 1 hour operation for each sensor node)

3. Results and discussion

In this work, we develop a non-cryptographic type of defense by checking the forwarding of the upstream nodes by overhearing their transmission. We consider Ad Hoc on demand vector routing protocol to implement these attacks.

In the Black Hole attack, a node will participate in routing but will drop all the packets it receive [11]. The malicious node will always advertise in the network that it has a fresher route to the destination by setting the sequence number to a large value and will reply to the broadcast route request packet before other nodes send a reply. Thus, the attacker node will attract all the traffic in its transmission range towards itself and then drop the packets. This type of situation will decrease the packet delivery ratio, but at the same time the energy of the black node will decrease rapidly resulting in self-immolation of the node. However, during the time of the data transmission the other nodes which send the packet to the black node will result in decrease of their energy due to repeated transmissions for the same packet. This will decrease their energy and result in reduced life cycle of the node. In Gray Hole attack, the attacker node drop selective packets according to some criteria or randomly [4]. This type of attack is difficult to detect, especially in wireless scenario where packets are dropped because of the congestion, channel capacity etc. This algorithm is based on the probability of attack which depends on the ratio of number of packets to the number of packets transmitted. If the probability of attack is greater than the probability of black hole attack and it is true twice then the attack is black hole attack and if the probability of attack is greater than the probability of gray hole attack and it is true twice then the

attack is gray hole attack. After the detection of the attack all the nodes are sent a broadcast not to include the node in any future routing for transmission of packets. The complete algorithm for different scenario is given as under:

Scenario: (As shown in Fig. 2)

Case 1: Homogeneous ad hoc or wireless sensor network

Wireless sensor network is a large network of sensors which have the ability to communicate with each other. These sensor nodes are transmitting the data from one sensor to another for further transmission to the sink node. In ad hoc networks Ad Hoc on demand vector is a source initiated advanced on demand routing protocol. Each sensor node has a routing table that stores the information of the next hop node to route the destination. When a source node wants to route a packet to sink node, it uses the specified route if a fresh route to the sink is not available otherwise it will update its table for shortest route by the route discovery using route request message to its neighboring nodes. In Gray-Hole attack the malicious node selectivity or randomly forwards packets passing through it. Sink node after receiving packet from the source node, unicast (route reply) message en-route neighboring node from which it receives the packet. In Black-Hole attack, the malicious node pretends as if it has the shortest path to the sink node and drops all the packets.

Case 2: Heterogeneous wireless sensor network with LEACH based cluster head

The wireless sensor network is partitioned into clusters and each cluster consists of a group of sensor nodes which may or may not transmit data to the destination via the neighboring nodes. Mostly, the nodes communicate directly with the cluster head. The cluster head is chosen which is having the maximum energy level amongst the cluster nodes. As in LEACH the process of selecting or electing a cluster head is repeated after a certain interval of time. The number of nodes in a cluster is less as compared to the case 1 [14]. But the Gray-Hole and Black-hole attack is possible if the nodes communicate with the cluster head via intermediate or neighboring nodes. Also, the attacks are possible if the node which acts as cluster head is compromised. The severity of the attack may be manifold as all the data packets from each and every node will be dropped.

Case 3: Heterogeneous wireless sensor networks with Advanced Node as cluster head

The wireless sensor network is partitioned into clusters as in case of case 2 but the cluster head is predefined and the advanced node which acts as a cluster head is presumed to have higher energy, processing power and range [5] as compared to the normal sensor nodes. The possibility of Gray-Hole and Black-Hole attacks is less as compared to the case 1 or case 2. As it will be difficult to compromise the cluster head which is responsible for the transmission of the data from the nodes to the gateway. All the nodes will directly communicate with the cluster head, but as a special case the nodes may also communicate with the cluster head via the intermediate or neighboring nodes within that cluster. In the earlier case, the probability of compromising a node is lesser. Also, it is possible to use the cryptographic algorithms like key exchange mechanisms between the nodes and the cluster head during data transmission.

4. Algorithm for detection and isolation of Byzantine nodes by non-cryptographic methods

In either case of Byzantine attacks, Gray-Hole or Black-Hole attack, the detection of the type of attack is first step. After we know the type of attack our next priority is to identify the compromised nodes in the network. The algorithm detects these nodes by non-cryptographic methods, checking the forwarding of the nodes by overhearing their transmission and isolation of these nodes so that cannot take part in routing. The scenario is shown in Fig. 2.

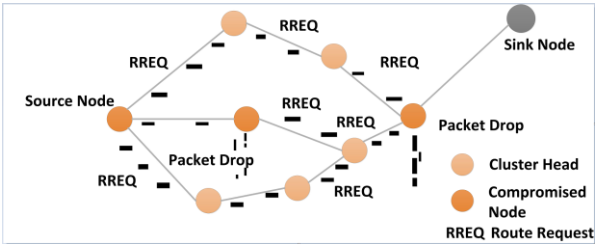

Fig. 2 Gray-hole and Black-hole attack detection and isolation scenario

4.1. Assumptions

Before the implementation of the algorithm we have taken certain assumption. Since there are many other factors which could cause the change in the throughput which we have taken as solely by the byzantine attacks. Like con-gestion due to buffer overflow is not insignificant, as we need to restrict the upstream node from delivering packets when the downstream node does not have sufficient space. (b) In practical cases black hole attack may not drop all the packets; it has its dependence on other factors as well. (c) As the signal power decreases the range is also decreased, but in case of WSN, the nodes are at a very short distances for a decrease in energy is not affected too much extend as compared to long distance communication. (d) In multi-hop communication each node maintains the table of the routing information during the transmission of packets, but here each node will be having additionally the attack table, this may add some overhead to the packets.

a. No packet is dropped due to buffer overflow
b. Black-Hole attack drops all the packets it receives
c. Range is not getting affected by decrease in the energy level of a node
d. Each node will maintain an attack table

Notation and parameters

n_{id}	Node identifier
n_t	Total no. Of packets transmitted by a node
n_d	Total no. Of packets dropped by a node
n_L	Total packet loss
$n_L = n_t - n_d$	
Pa	Probability of packets successfully received
Pb	Probability of presence of Black-Hole
Pg	Probability of presence of Gray-Hole
$Pa = n_L / n_t$	
N_r	Reporter node
N_A	Attacker node
CH	Cluster Head
C_{id}	Cluster id

4.1.1. Algorithm for homogeneous network

For a particular interval:

1. Calculate value of n_L
   $n_L = n_L - n_d$;
2. Define values of Pb and Pg //Threshold values as per the scenario
3. Calculate Pa
   $P_a = n_L / n_t$;
4. If (Pa >= 2Pb){
   Then broadcast packets to all Ns and Rs with nid of both reporter node and attacker node.
   Type –of-attack = B;}
   else if (Pa >= 2Pg){
   Broadcast packets to all Ns and Rs with nid of both reporter node and attacker node.
   Type-of-atack = G;}
   Else if (Pa>Pg and Pa >Pb){
   Broadcast packets to all Ns and Rs with nid of both reporter node and attacker node.
   Type-of-attack = G;}
   Else{
   Print("No attacker node found"); and broadcast nid of sender node to all Ns and Rs".
   Type-of-attack = nil;}

4.1.2. Algorithm dedicated cluster head

Assumption is that cluster heads are pre assigned with identified cluster nodes. For a particular cluster and for a particular interval:

1. Assign a node CID with maximum power
2. Calculate value of nL for that particular cluster
   nL = nt – nL;
3. Define value of Pb and Pg for a cluster
4. Calculate Pa
   Pa = nL/nt;
5. If (Pa >= 2Pb){
   Broadcast packets to all Ns, rs and CH with nid of both Nr and NA
   Type-of-attack = B;}
   Else if (Pa >= 2Pg){
   Broadcast packets to all other Ns, Rs and CH with nid of both Nr and NA
   Type-of-attack = G;}
   Elseif (Pa >Pg and Pa >Pb){
   Broadcast to all Ns, Rs and CHs of cluster with nid of both Nr and NA
   Type-of-attack = G;}
   Else{
   Print ("No attack found")

4.1.3. Algorithm Heterogeneous Network

Assumption is that network is divided into clusters <=100. For a particular cluster and for a particular interval:

1. Choose a node randomly as CH and assign Cid
2. Calculate value of nL for that particular cluster
   nL = nt – nd;
3. Define value of Pb&Pg for a cluster.
4. Calculate Pa
   Pa = nL/nt;
5. If (Pa >= 2Pb){
   If (attacker nid = Cid of CH){
   Broadcast packets to all other CHs with Cid of attacker CH
   Type-of-attack = B;}
   Else {
   Broadcast packets to all Ns, Rs and CH with nid of both Nr& NA.
   Type-of-attack = B;}
   Elseif(Pa>= 2Pg){
   if (attacker nid = Cid) {
   Broadcast packets to all CHs with Cid of attacker CH
   Type-of-attack = G;}
   Else{
   Broadcast packets to all Ns and Rs and to CH of cluster with nid of both Nr and Na
   Type-of-attack = G;} }
   Else if (Pa>Pg and Pa>Pb){
   If(attacker nid = Cid){
   Broadcast packets to all other CHs with Cid of attacker CH
   Type-of-attack = G;}
   Else{
   Broadcast packets to all Ns, Rs& CH with nid of both Nr and na
   Type-of-attack = G;} }
   Else{
   Print("No attack found"); and broadcast
   nid of sender node to all Ns, Rs and CHs
   Type-of-attack = Nil;
   }

5. Results based on the algorithm for detection and isolation

From the simulation results as is evident from the Fig. 4 throughput vs. time. Initially, we simulate the network with no attack; the throughput is 90-95%. Then, as we introduce the black hole attack in the network, throughput decreases to 3%-5%. Now, as the network uses the isolation algorithm, throughput increases to 67%. Similarly in

case of gray hole attack, initially we simulate the network without attack and the throughput is 90-95%. Then, we introduce the gray hole attack and the throughput decreases to 35%-50%. After using the isolation algorithm the throughput increases to 88%.

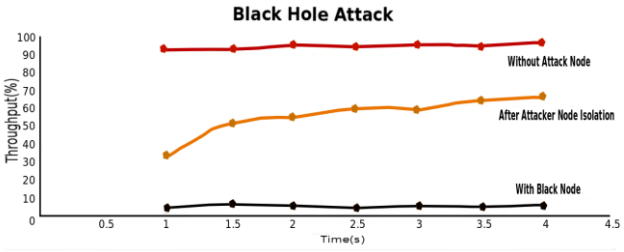

Fig. 3 time(s) vs. throughput (%)

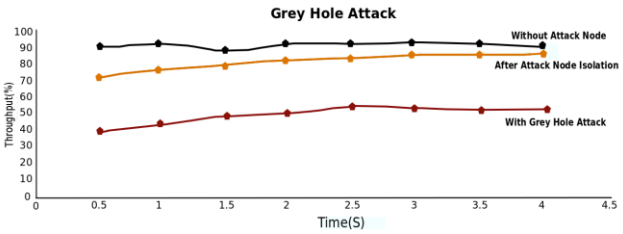

Fig. 4 time vs. throughput (%)

6. Conclusion

As shown in Fig. 3 and Fig. 4, there is remarkable improvement in the throughput after using the proposed al-gorithm for isolation of the malicious nodes. The algorithm will be more suited to the applications were we require to have energy efficient design. Since the algorithm is a non-cryptographic one and purely depend on the probability of packets successfully received, therefore probability of presence of black hole nodes and probability of presence of gray hole nodes may vary in some cases. But the algorithm will be useful for the sensor networks where we can't use the cryptographic algorithms to tackle the security problem due to the fact that increased processing and communication time will increase the energy consumption.

If we partitioned the network into clusters then the gray hole or the black hole attack will remain confined to its own cluster only without affecting the other clusters in the network till the cluster head itself is not compromised. But if we use the advanced node in the network as a cluster head then the probability of cluster head to be compromised will be lesser due to the fact that the node is predefined cluster head and we can also use the cryptographic mechanisms like the key exchange etc. for secure transmission with the processing to be done centrally at the cluster head (Advanced node), as it is having higher processing, communication and energy as compared to the member nodes of the cluster.

References

[1] A. Perrig, J. Stankovic, and D. Wager, "Security in wireless sensor networks," Communication of the ACM, vol. 47, no. 6, pp. 53-57, June 2004.

[2] D. Estrin, R. Govindan, and J. Heidemann, S. Kumar, "Next century challenges: scalable coordination in sensor networks," Proc. ACM International Conf. Mobile Computing and Networking, ACM Press, 1999, pp. 263-270.

[3] Y. Yu, B. Krishnamachari, V. K. Prasanna, "Energy-latency tradeoffs for data gathering in wireless sensor networks," Proc. IEEE Computer and Communication Societies, IEEE Press, 2004.

[4] S. E. Khediri, N. Nasri, A. Wei, and A. Kachouri, "A new approach for clustering in wireless sensors networks based on LEACH," Procedia Computer Science, vol. 32, pp. 1180-1185, 2014.

[5] S. A. Sofi and R. Naaz, "Energy efficient routing protocol for structured deployment of wireless sensor networks," International Conf. Next Generation Networks, IET Press, September 2010, p. 10.

[6] S. Sofi, E. Malik, R. Baba, H. Baba, and R. Mir, "Analysis of byzantine attacks in ad hoc networks and their mitigation," International Conf. Computing and Information Technology, February 2012, pp.794-799.

[7] W. Li and A. Joshi, "Security issues in mobile ad hoc net works - a survey," https://pdfs.semanticscholar.org/b221/99c61df5445836c5f1bbd0ea6f02dabefd6b.pdf, 2007.

[8] Y. C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks in wireless ad hoc network routing protocols," Proc. 2nd ACM workshop on Wireless security, ACM Press, 2003, pp. 30-40.

[9] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad hoc networks, vol. 1, no. 2, pp. 293-315, 2003.

[10] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad-hoc networks," Proc. 6th Annual International Conf. Mobile Computing and Networking, pp. 255-265, August 2000.

[11] H. Li, K. Li, W. Qu, and I. Stojmenovic, "Secure and energy efficient data aggregation with malicious aggregator identification in wireless sensor networks," Future Generation Computer Systems, vol. 37, pp. 108-116, 2014.

[12] Y. Zhao, Y. Zhang, Z. Qin, and T. Znati, "A co-commitment based secure data collection scheme for tiered wireless sensor networks," Journal of Systems Architecture , vol. 57, no. 6, pp. 655-662, 2011.

[13] Manju, S. Chand, and B. Kumar, "Improved-coverage preserving clustering protocol in wireless sensor networks," International Journal of Engineering and Technology of Innovation, vol. 6, no. 1, pp. 16-29, 2016.

[14] R. Duche and N. Sawade, "Energy efficient fault tolerant sensor node failure detection in WSNS," International Journal of Engineering and Technology of Innovation, vol. 6, no. 3, pp. 190-210, 2016.

[15] M. Abdelhakim, L. E. Lightfoot, J. Ren, and T. Li, "Distributed detection in mobile access wireless sensor networks under byzantine attacks," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 4, pp. 950-959, April 2014.

[16] M. Young and R. Boutaba, "Overcoming adversaries in sensor networks: a survey of theoritical models and algorithm approaches for tolerating malicious interferences," IEEE Communications Survey and Tutorials, vol. 13, no. 4, 2011.

