hardware, topology change, environment and power consumption.

[2] The focus is on routing security in wireless sensor networks. Current proposals for routing protocols in sensor networks optimize for the limited capabilities of the nodes and the application specific nature of the networks, but do not consider security. Although these protocols have not been designed with security as a goal, it is important to analyze their security properties. When the defender has the liabilities of insecure wireless communication, limited node capabilities, and possible insider threats, and the adversaries can use powerful laptops with high energy and long range communication to attack the network, designing a secure routing protocol is non-trivial. One aspect of sensor networks that complicates the design of a secure routing protocol is in-network aggregation. In more conventional networks, a secure routing protocol is typically only required to guarantee message availability. Message integrity, authenticity, and confidentiality are handled at a higher layer by an end-to-end security mechanism such as SSH or SSL. End-to-end security is possible in more conventional networks because it is neither necessary nor desirable for intermediate routers to have access to the content of messages. In sensor networks, in-network processing makes end-to-end security mechanisms harder to deploy because intermediate nodes need direct access to the content of the messages. Link layer security mechanisms can help mediate some of the resulting vulnerabilities, but it is not enough.

Wormhole attack is introduced [3]. It is a severe attack that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. A general mechanism, called packet leashes, for detecting and thus defending against wormhole attacks is presented in this paper, and a specific protocol, called TIK, that implements leashes.

In multihop wireless systems, such sensor networks, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security attacks. A particularly devastating attack is known as the wormhole attack, where a malicious node records control and data traffic at one location and tunnels it to a colluding node, which replays it locally. This can have an adverse effect in route establishment by preventing nodes from discovering routes that are more than two hops away. [4] A lightweight countermeasure for the wormhole attack, called LITEWORP, which does not require specialized hardware is discussed. LITEWORP is particularly suitable for resource-constrained multihop wireless networks, such as sensor networks. This allows detection of the wormhole, followed by isolation of the malicious nodes.

Large-scale peer-to-peer systems face security threats from faulty or hostile remote computing elements. To resist these threats, many such systems employ redundancy. If a single faulty entity can present multiple identities, it can control a substantial fraction of the system, thereby undermining this redundancy. One approach to preventing these "Sybil attacks" is to have a trusted agency certify identities. [5] Shows that, without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities.

In a large-scale sensor network individual sensors are subject to security compromises. A compromised node can inject into the network large quantities of bogus sensing reports which, if undetected, would be forwarded to the data collection point (i.e. the sink). Such attacks by compromised sensors can cause not only false alarms but also the depletion of the finite amount of energy in a battery powered network. [6] A Statistical En-route Filtering (SEF) mechanism that can detect and drop such false reports is presented. SEF requires that each sensing report be validated by multiple keyed message authentication codes (MACs), each generated by a node that detects the same event. As the report is forwarded, each node along the way verifies the correctness of the MACs probabilistically and drops those with invalid MACs at earliest points. The sink further filters out remaining false reports that escape the en-route filtering. SEF exploits the network scale to determine the truthfulness of each report through collective decision-making by multiple detecting nodes and collective false-report-detection by multiple forwarding nodes.

[7] Describes an Intrusion-tolerant routing protocol for wireless Sensor Networks (INSENS). INSENS constructs forwarding tables at each node to facilitate communication between sensor nodes and a base station. It minimizes computation, communication, storage, and bandwidth requirements at the sensor nodes at the expense of increased computation, communication, storage, and bandwidth requirements at the base station. INSENS does not rely on detecting intrusions, but rather tolerates intrusions by bypassing the malicious nodes. An important property of INSENS is that while a malicious node may be able to compromise a small number of nodes in its vicinity, it cannot cause widespread damage in the network.

Selective forwarding attacks may corrupt some mission-critical applications such as military surveillance and forest fire monitoring in wireless sensor networks. In such attacks, most of the time malicious nodes behave like normal nodes but will from time to time selectively drop sensitive packets, such as a packet reporting the movement of the opposing forces, and thereby make it harder to detect their malicious nature. [8] CHEMAS (Checkpoint-based Multi-hop Acknowledgement Scheme), a lightweight security scheme for detecting selective forwarding attacks has been proposed. This scheme can randomly select part of intermediate nodes along a forwarding path as checkpoint nodes which are responsible for generating acknowledgements for each packet received. The strategy of random-checkpoint-selection significantly increases the resilience against attacks because it prevents a proportion of

the sensor nodes from becoming the targets of attempts to compromise them. In this scheme, each intermediate node in a forwarding path, if it does not receive enough acknowledgements from the downstream checkpoint nodes, has the potential to detect abnormal packet loss and identify suspect nodes.

3. Problem Definition

To build a secure and an efficient mechanism for intrusion prevention in wireless sensor network.

4. Proposed Work

The assumptions in the proposed method are as follows. Each node x shares a symmetric key K_X with the BS, and it can derive the encryption key K_{XE} and the MAC generation key K_{XM}. The topology and routing path of the entire network are constructed. A sensing node generates and forwards an event report to the BS and the network topology and routing path is reconstructed. BS and every node in the network communicate with each other using the topology and route construction message (TRC message) and the neighbor information response message (NIR message). The TRC message has the following form:

TRC||IDx||OHCTRC||MAC(KeyXm,TRC||IDx||OHC||MACparent)

TRC is a message type and IDx is the sending node's ID. OHC is a one-way hash chain number generated by BS. This is used to prevent malicious reuse of the TRC message by an intruder. MAC_{parent} is the MAC generated by the parent of sender. BS broadcasts the first TRC message within the transmission range. Each receiving node records the sender in its neighbor list. If the sender is the first node from which it receives a TRC message in the current round, it records the sender as its parent node. After that, these nodes modify the ID_x and MAC of the TRC message and re-broadcast this TRC message. Figure 1 describes this phase.

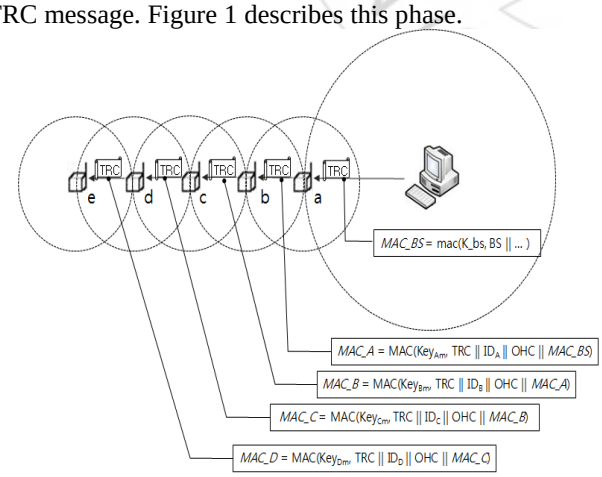

Figure 1: Broadcast of TRC message and nested MAC

After all the nodes receive a TRC message, each of them generates a neighbor information respond (NIR) message and sends it to the BS. The NIR message has the following form:

NIR || IDX | |E (KXe, NInfo) || MAC (KeyXm, OHC||NIR||IDX|| E (KeyXe, NInfo))

NInfo indicates the neighbor node information of the sender, E (K_{Xe}, NInfo) is the encrypted NInfo by using the encryption key K_{Xe}. The NIR messages are forwarded to BS. BS obtains neighbor node information from the NIR messages, and constructs the network information table as shown in figure 2.

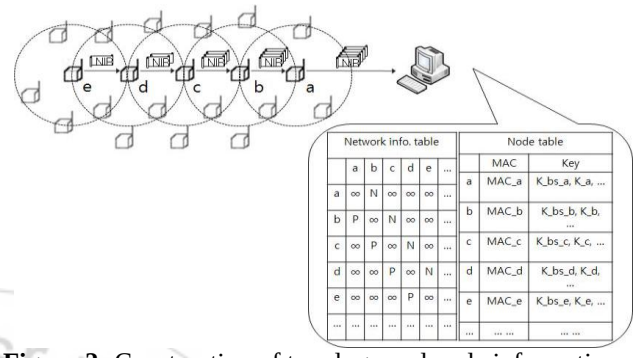

Figure 2: Construction of topology and node information at BS

After the network topology is complete, the BS computes the routing path and makes a routing table for each node. The routing path is composed of the main path and report/fallback path. The main path is used to transmit the sensing data, while the report/fallback path is used when control messages are transmitted, such as an alert message that implicates the malicious node. The report/fallback path may also be used when the main path is damaged. Computed paths are reorganized by the routing table of each node. The BS sends a routing table to each node using the routing table update message (RTU message) by unicast in a breadth-first manner. The RTU message has the following form:

RTU || OHCRTU || RT<dest, src, immediate_sender>

The routing table of each node is composed of RT<dest, src, immediate_sender> in the RTU message. The three elements in RT are the destination node, source node, and immediate sending node.

a sensing node generates and forwards an event report to the BS. During the forwarding process, some nodes on the path are randomly selected as check nodes. The event message (EV message) has the following form:

RInfo || msg_ID || CHK_seed || payload

RInfo of EV messages is the routing information. CHK_seed is a seed value for probability function Fprob() that was previously loaded into the memory of the receiving node. The output of Fprob() becomes one with certain probability and if the output is one, the receiving node becomes a check node. A check node sends back an ACK message in direction to the source node. The ACK message has the following form:

RInfo || ACK || ack_m_ID || MAC(KXm, ACK|| ack_m_ID) ||TTL

The ACK message is forwarded limited number of hops, the time to live (TTL) value. If TTL is one, an ACK message is forwarded to the next check node in direction to the source node. Sensor nodes that forwarded an event report but not received sufficient number of ACK messages transmit an ALERT message to the first check node in direction to the source node. The ALERT message has the following form:

RInfo || ALERT || P_ID || L_M_ID || MAC (K_{Xm}, ALERT|| P_ID ||L_M_ID)

Alert message sending node selects one of its parent nodes and adds this information to the ALERT message. P_ID indicates the ID of the prosecuting node that creates the ALERT message. L_M_ID indicates the ID of a lost message. The first check node that receives ALERT messages transmits the ALARM message using the fallback path to report the damage that occurred in the main path. The ALARM message has the following form:

RInfo || ALARM || P_ID_list || lost_payload || MAC (K_{Xm},ALARM || P_ID_list || lost_payload)

The network topology and routing path is reconstructed. However, initial construction phase do not have to be repeated, since BS obtains the path and node information in the sensing data transmission phase. More specifically, ALERT and ALARM messages offer the information necessary to update the path and network topology information. BS selects a path and modifies the topology and routing tables. Figure 3 shows the routing information update in BS.

5. Simulation Model and Parameters

Network Simulator 2 is used to simulate proposed method. The simulation is done for 20 to 140 nodes in which control overhead, normalized overhead and average energy consumption simulation parameters are considered. In simulation, 50 to 140 mobile nodes move in a 1000 meters x 1000 meters rectangular region.

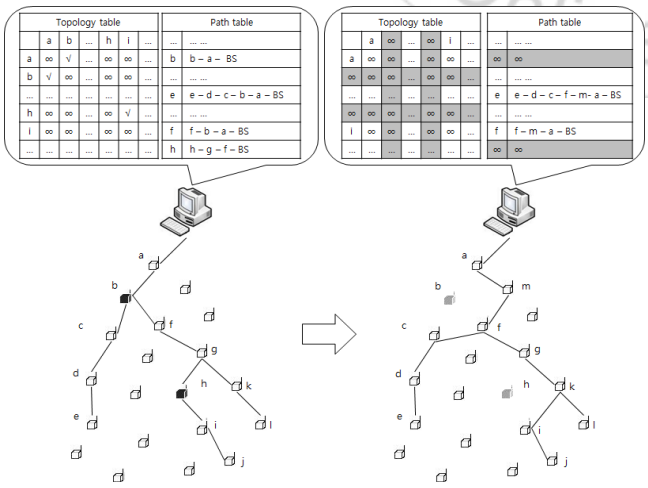

Figure 3: Routing table update at BS.

6. Result Graphs

Figure 4 shows the graph of number of nodes versus normalized overheads in which overheads decreases as the total number of increases this is because of our security mechanism implemented for the wireless network. Figure 5 shows graph for the number of nodes versus control overheads. Figure 6 shows the graph of number of nodes versus average energy consumption in which we can see that the energy decreases as the number of nodes are increased.

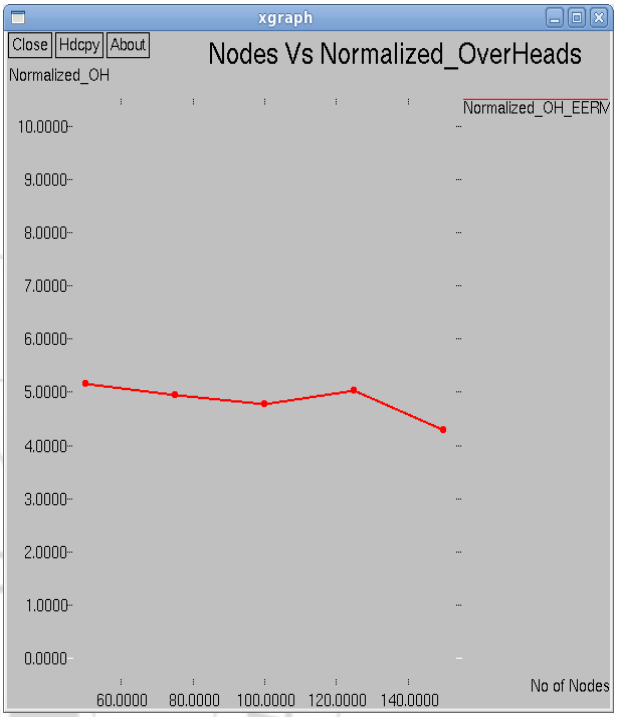

Figure 4: Nodes Vs Normalized overheads

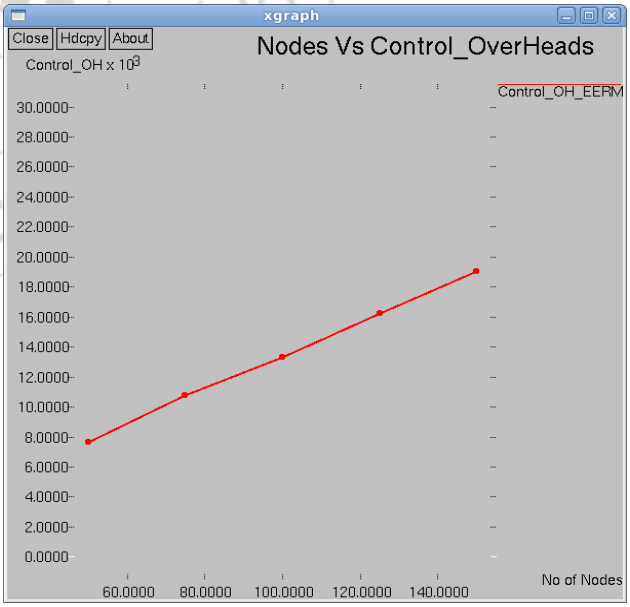

Figure 5: Nodes Vs Control Overheads

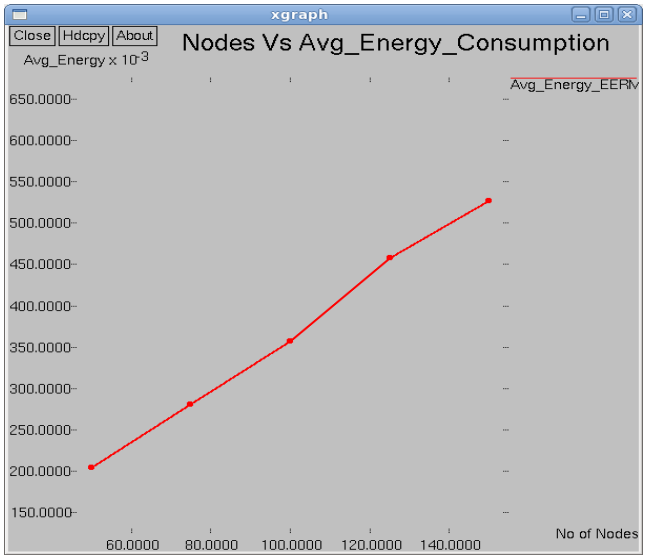

Figure 6: Nodes Vs Average energy consumption

7. Conclusion

The proposed method is energy efficient security mechanism for wireless network. A method is proposed which is energy efficient in the environment where both intrusion detection and prevention are used in WSNS. The attacks occurring in WSN are alternative and simultaneous which cannot be predicted. Therefore there is need for intrusion detection and prevention. The proposed method is for both intrusion detection and prevention. Also the communication overheads and energy consumption are reduced as shown in the simulation results.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," Communications magazine, IEEE, vol.40, no.8, pp.102-114.
[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks:Attacks and countermeasures," Ad hoc networks, vol.1, no.2, pp.293-315.
[3] Y. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks,"INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, pp.1976-1986.
[4] I. Khalil, S. Bagchi, and N. B. Shroff, "LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks, "Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on, pp.612-621.
[5] J. R. Douceur, "The sybil attack," in Peer-to-peer SystemsAnonymous , pp.251-260, Springer, 2002.
[6] B. Xiao, B. Yu, and C. Gao, "CHEMAS: Identify suspect nodes in selective forwarding attacks," Journal of Parallel and Distributed Computing, vol.67, no.11, pp.1218-1230, 2007.
[7] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," Comput.Commun., vol.29, no.2, pp.216-230, 2006.
[8] Fan Ye, Haiyun Luo, Songwu Lu, and Lixia Zhang, "Statistical en-route filtering of injected false data in sensor networks," IEEE Journal on Selected Areas in Communications, vol.23, no.4, pp.839-850, 2005.