SECURE AND EFFICIENT DATA TRANSMISSION USING M-SPIN PROTOCOL FOR CLUSTER-BASED BASED WIRELESS SENSOR NETWORKS

D.Ranjitha[1], Dr.A.Marimuthu, M.C.A.,M.Phil.,M.B.A(Systems),Ph.D.,[2]

[1] *M.Phil Research scholar, Post graduate and Research Department of Computer science, Government Arts College, Coimbatore, Tamil Nadu, India*

[2] *Associate Professor, Post graduate and Research Department of Computer science, Government Arts College, Coimbatore, Tamil Nadu, India*

ABSTRACT

Sensor networks are recently rapidly growing research area in wireless communications and distributed network. Data transmission is one of the major challenges in wireless sensor network. Different routing protocols have been proposed to save energy during data transmission in WSN. Since the nodes in Wireless Sensor Networks (WSN) are typically very small in size and are powered by irreplaceable battery, efficient use of energy becomes one of the most challenging tasks while designing any protocol for WSN. The proposed algorithm for increasing energy efficiency of routing protocol M-SPIN belonging to SPIN family protocol. Routing protocol makes the transmission in an efficient manner and ensures reliable delivery over multiple-hop relay in WSN. A secure data transmission for cluster based WSNs (CWSNs), where the clusters are formed dynamically and periodically. The existing two secure ands efficient data transmission(Set) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature(IBS) scheme and the Identity-based Online/Offline digital Signature(IBOOS) scheme, respectively.

A SET-IBS and SET-IBOOS protocol are the existing protocols which show the feasibility with respect to the security requirements and security analysis against various attacks. When compared to existing protocol, the M-SPIN takes minimum amount of time for data transmission and high protocol accuracy. The results shows that the proposed protocols have better performance than existing protocols for CWSNs, in terms of security overhead, protocol accuracy and energy consumption.

Keyword: *Wireless Sensor Networks*, I*dentity-Based digital Signature (IBS), Identity-Based Online/Offline digital Signature (IBOOS), Modified Sensor Protocol for Information via Negotiation (M-SPIN).*

1. Wireless device Network

A wireless sensor network is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions such as sound, temperature and motion. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN [1]. Efficient data transmission is one of the most important issues for WSNs.

1.1Existing Work

The existing IBS scheme and IBOOS scheme used that the conventional schemes are not specifically designed for CWSNs. It adapts the conventional IBS scheme for CWSNs by distributing functions to different kind of sensor nodes. There is no protocol accuracy in SET-IBS and SET-IBOOS. It takes more time for data transmission.

2 Proposed work

Another fascinating truth is that energy consumption not solely depends on sensing knowledge the information however additionally on process the perceived data and sending or receiving them to or from its neighbor nodes. Therefore if it's potential to manage range of transmission and receipt of messages, a big quantity of energy is saved. Figure1 shows an M-SPIN, within the WSN divides the whole network into 2 regions, A and B. Detector nodes in region A area unit on the opposite facet within the network as compared with the sink node and detector nodes in region B area unit on constant facet and nearer to the sink node. Detector nodes of region A will receive knowledge from the event node; however, they're going to unnecessarily waste their energy in receiving or sending the information. So as to succeed in knowledge to the sink node, knowledge can ought to travel a lot of hops if they're sent via the nodes in region A. Thus, once a happening happens, it's continually fascinating that the info is distributed through the nodes in region B. this might save the energy spent for transmission of a bit of information from a happening node to the sink node. However, such selective transmission isn't supported within the existing protocols. To beat this downside, we tend to propose an MSPIN protocol. In few applications like alarm observation applications want fast and reliable responses. Suppose in fire warning system, fast response is required before any disaster happens. During this case, it's fascinating that knowledge should be disseminated towards the sink node terribly quickly. MSPIN [7] routing protocol is healthier approach for such form of applications than existing protocols.

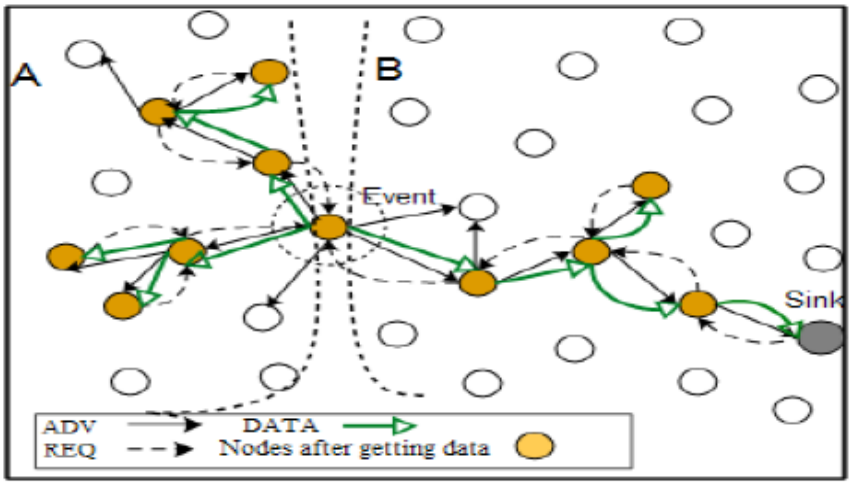

Fig -1 M-SPIN Protocol

In our planned protocol, we tend to add a replacement part referred to as Distance discovery to search out distance of every detector node within the network from the sink node in terms of hops. This suggests that nodes having higher worth of hop distance area unit far-off from the sink node. Different phases of M-SPIN area unit Negotiation and knowledge transmission. On the idea of hop distance, Negotiation is finished for causing an actual knowledge. Therefore, use of hop worth controls dissemination of information within the network. Finally, knowledge is transmitted to the sink node.

2.1 Distance discovery

Hop distance is measured from sink nodes. Initially the sink node broadcasts Startup packet within the network with kind, nodeid and hop. Here kind means that form of messages. The node id represents id of the sending node and hop represents hop distance from the sink node. Initial worth of hop is about to one. Once a detector node receives the Startup packet, it stores this hop worth as its hop distance from the sink node in memory. Once storing the worth, the detector node will increase the hop worth by one so re-broadcast the Startup packet to its neighbor nodes with changed hop worth. It's going to even be potential for a detector node to receive multiple Startup packets from totally different intermediate nodes. Whenever a detector node b receives Startup packets from its neighbours ai, $1 \leq i \leq n$, it checks the hop distances and set the space to the minimum. This method is sustained till all nodes within the network get the Startup packets a minimum of once inside the space discovery part. After completion of

this part, next part are started for negotiation. StartupMsg structure contains 3 member variables. Hop Table structure contains just one member referred to as hop_t to store the hop worth at every node.

2.2 Negotiation

The supply node sends an ADV message. Upon receiving an ADV message, every neighbor node verifies whether or not it's already received or requested the publicized knowledge. Not solely that, receiver node additionally verifies whether or not it's nearer to the sink node or not as compared with the node that has sent the ADV message. If hop distance of the receiving node (own_hop) is a smaller amount than the hop distance received by it as a part of the ADV message (rcev_hop), i.e. own_hop < rcev_hop, then the receiving nodes send REQ message to the causing node for current knowledge. The causing node then sends the particular knowledge to the requesting node exploitation knowledge message. As before long as a node gets knowledge either from its own application or from different detector nodes, it stores that knowledge in its memory exploitation the operate storepkt. Additionally it uses set Current operate to specify that knowledge is presently residing in its memory. Once ADV message is received, then every receiving node 1st checks its record to determine whether or not it already has seen that knowledge exploitation the operate chkHistory. Moreover, it calls set Desired to point that knowledge packet it's looking forward to. The supply nodes that receive the REQ use the operate get Current. It helps to see whether or not they received REQ is for the hold on knowledge specific by the set Current operate that the node has sent the ADV. once a requesting node receives any knowledge, it like a shot checks whether or not the info is that the same that it's sent the request exploitation getDesired operate. The info packet contains the hop distance worth at the side of the data regarding the event.

2.3 Data Transmission

Knowledge transmission part is same as SPIN-BC protocol. Once request is received by the supply node, knowledge is straight away sent to the requesting node. If the requesting nodes area unit intermediate nodes aside from the sink node then the Negotiation part repeats. Thus, the intermediate detector nodes broadcast ADV for the info with changed hop distance worth.

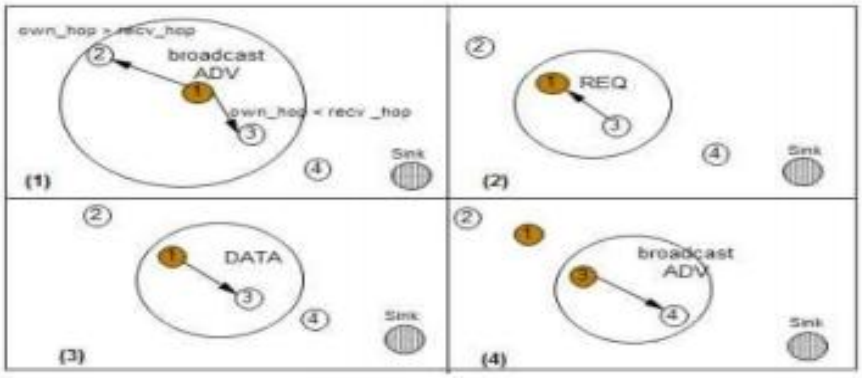

Fig2-Data transmission of M-SPIN Protocol

The causing nodes modify the hop distance field with its own hop distance worth and add that in packet format of the ADV message. The method continues until knowledge reaches the sink node. Figure five illustrates Negotiation and knowledge transmission part. The M-SPIN protocol. (1) Node one starts advertising its knowledge to any or all of its neighbours. (2) Node three responds by causing letter of invitation to node one. (3) once receiving the request, node one sends the info. (4) Node three once more sends promotional material bent its neighbours for the info that it received from node one.

M-SPIN features already been enforced however it still has a downside of energy as many nodes area unit traversed multiple times which ends in elimination of these nodes from the network. To unravel this downside we'll use the energy of the nodes as a parameter. This sort of technique has already been utilized in the SPIN-EC protocol. Within the SPIN-EC protocol we tend to were victimization energy issue. During this if a node doesn't have

sufficient energy for collaborating within the knowledge transmission, therein case it solely accepts the publicized knowledge however doesn't forward the message to their neighboring nodes.

Solely within the case if a node has sufficient energy, it might participate in communication otherwise it saves its energy just for its own transmission. To implement our planned algorithmic program, we tend to area unit playing some changes. First off we tend to add energy as a parameter. The worth of the energy parameter of the node is capable the battery lifetime of the node. We tend to additionally outline a Threshold Energy for the node. If the worth of the energy parameter is larger than the brink energy, that node has active participation within the network.

3. Result

3.1 Protocol Accuracy Chart

When compared to SET-IBS,SET-IBOOS, the proposed protocol M-SPIN having high accuracy.

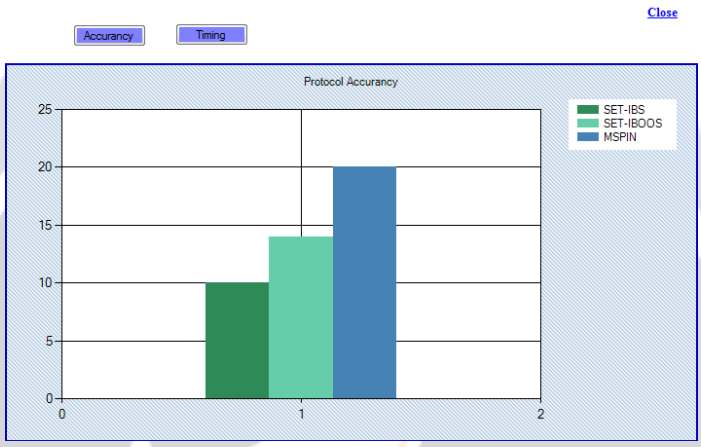

Chart -1: Protocol Accuracy chart

3.2 Time Taken Chart

The M-SPIN protocol takes less time for data transmission than SET-IBS and SET-IBOOS protocol.

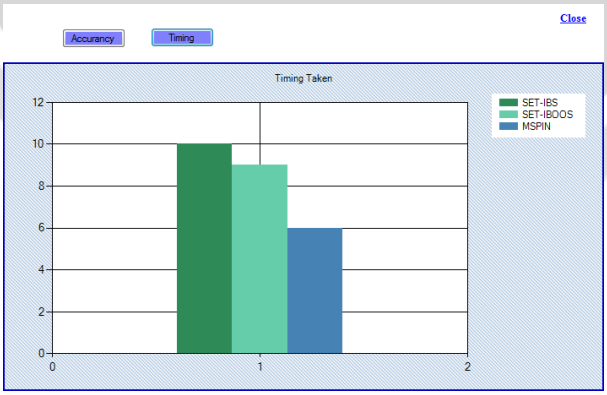

Chart -2: Time taken chart

4. Conclusion

According to this projected algorithmic program Energy potency of the nodes is enhanced as a result of energy state issue antecedently confirm the energy state of the nodes, if they need no adequate energy to participate within the transmission of information in this case they conserve their energy just for their use and stay exist within the network. Second it conjointly facilitate in providing the alternate path for knowledge transmission as some nodes area unit traversed multiple times just in case of the M-SPIN. However currently by deciding the energy state the

trail is pleased. At the side of this it's some limitation just like the complicated computation suggests that hard the energy state at every node at anytime could be a robust task. We've got to calculate it at anytime if just in case it cannot be calculated then it's terribly tough to implement it and it works same as that of M-SPIN protocol.

5. References

[1]. T. Hara, V. I. Zadorozhny, and E. Buchmann, Wireless Sensor NetworkTechnologies for the Information Explosion Era,Stud. Comput.Intell.Springer-Verlag, 2010, vol. 278.

[2]. Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, 2006.

[3]. A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, pp. 2826–2841, 2007.

[4]. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, 2002.