IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 99-103
www.iosrjournals.org

Enhancing the Lifetime and Improving the Security of the Smart Mines

Meera G S[1], Kavitha Karun A [2]
[1, 2]*Computer Science Dept, Lourdes Matha College of Science and Technology/ Kerala University,India*

ABSTRACT: *Mostof the WSN applications are designed to overcome the limitations pertaining to the sensor nodes. To enhance the life of the network, the power of the sensor nodes needs to be recharged as required. The paper proposes an inductive recharging to enhance the life of smart mines by exploring the area of the network using multiple mobile nodes. We propose a role-based exploration technique to explore the area for recharging mobile nodes. To enhance the MAC level security, against jamming attack caused by interference of other signals, we adopt frequency hopping MAC protocol which is achieved by time-synchronizing all the smart mines deployed.*

Keywords *-WSN, Frequency hopping, Inductive recharging, Area exploration*

I. INTRODUCTION

Wireless Sensor Networks gained a lot of research interests in the recent past due to its applications such as monitoring and tracking. Sensor nodes used in WSN are equipped with more than one sensors, a processor, a memory and a radio for communication. WSN has lots of applications in the areas of environmental, military, health-care monitoring and tracking [1]. The nodes in the sensor network will sense various physical phenomena like temperature, light intensity, sound etc. and send the sensed data to a base station or a sink node for further processing. WSN has lots of limitations in terms of memory, processing and computing facilities. These limitations make it less energy efficient and hence reduce the lifetime of the network. Most of the applications in WSN should be thus designed in such a way to overcome such limitations.

In most of the sensor network applications, sensor nodes once deployed, the manual intervention is not possible. It is not possible to replace the power source on depletion of battery. Energy consumed for communication is usually higher when compared to sensing and processing. As a result sensor nodes die, which in turn cause network failure and hence collapsing the overall communication. The lifetime of a sensor node can be increased by implementing an energy efficient protocol.

One of the deadly legacies of the 21-th century is the use of land-mines in warfare [2]. Land-mines are highly explosive self contained devices, which are laid into the ground, will explode when sufficient amount of pressure is applied on it. Based on the pressure applied, the land-mines can be classified as anti-personnel landmine or anti-tank landmine. Land-mines are deployed to secure disputed borders or to prevent the intrusion of enemy in the time of war. They continue to provide tragic and unintended consequences, even after a war has been ended. Since the location of the land-mines is not known even to those who have planted them, the demining has become a difficult task and is one of the major research issues for army and W.H.O. Even-though lots of conventional techniques are currently available for demining, automating the process of activation and deactivation of mines would yield better control of the mines.

Bharat et.al [2] propose the use of smart mines which are capable of activation/deactivation using a command driven from the base station or through the detection of sound signal. The paper implemented the smart mine using mutual authentication, creating a session, tasks and battery level monitoring functions. To provide a secure architecture for the smart mines, a Tiny ECC based PKI system was used which will authenticate the message passed between smart mines and the base station. Smart mines were designed in such a way that the power consumption was minimum. But if the network capacity is large, the idea of low power consumption is not guaranteed. The power could not be recharged if depleted.

This paper proposes a more secure way of communication by enhancing the life time of the smart mines using mobile nodes . We propose frequency hopping technique, which will help to prevent the jamming attack caused by the interference of other signals [4]. The frequency hopping technique is done over time synchronizing the sensor nodes in the field. This will provide a more securable communication between the smart mines and the base stations.

Section 2 describes the background work in detail. Section 3 describes the proposed approach. Section 4 Implementations and the future plan and conclude the paper.

II. BACKGROUND

Most of the existing work on wireless sensor network deals with improving the energy efficiency of the sensor nodes and thereby improving the network life time. Various protocols could be designed in such a way that will assure the network with reliability, low power consumption and cost reduction. The wireless sensor networks are highly resource constraint ad-hoc networks, which have limited memory, processing and computing capabilities.

In this paper, we are proposing a MAC level protocol for secure communication as well as mobile robots based wireless charging to improve the smart mine's life time. The main objective of smart mines [2] is to help military in deactivating the mines deployed in the field after the war. A possible way to achieve this objective, is by using sensor networks, which have proved to be successful in military applications like battlefield surveillance, tracking the position of the enemy, safeguarding the equipment on the side deploying sensors etc [1]. Integrating sensor networks with landmines will act as a potent force multiplier which can enable the landmines to be dynamic and be securely controlled by troops on the ground. Landmines are used to act as delay tactics for any enemy movement. Presently not much work has been done in order to wirelessly control the landmines; neither for de-mining them nor for controlling them whenever they are required. [2] focuses on achieving these objectives and additionally ensures secure wireless communication. The landmines are controlled by integrating them with sound sensors and actuator circuits, using wireless sensor devices. For reliable communication, hybrid cryptography is implemented using TinyECC based Public Key Cryptography (PKC) and Trivium based symmetric cipher.

The static smart mines once deployed can only be accessed or demined once the war is over. The smart mines are deployed in a region where there is no human intervention at all. The power consumption of the smart mines will be depleted over time. The power consumption of the nodes will be high even though the system is designed to minimize the power as the network capacity grows due to communication overhead. Power is required in the sensor mote for sensing, processing and communication. In most of the applications the power consumed during sensing and processing is comparatively less as compared to communication. The approach proposed in [2] is implemented in low profile Berkeley motes. Since the computational complexity of TinyECC is high, executing a single session will take more than ten seconds. For a long term deployment, such complex computation will cause unnecessary delay in communication and more over energy spend on computation will gradually increase. Attaching additional sensor such as acoustic sensors and actuator sensors will also consume energy and hence the overall life of the sensor network reduces. In real time applications, the use of a large number of static nodes will consume sufficient amount of power and hence recharging the smart mines is one of the major issues pertaining to static nodes.

The approach proposed in [2] has implemented a secure architecture for securing the sensitive information transferred between base station and the smart mine. Still, there can be security issues relating to the physical transmission of data between smart mine and the base station. The intruders can sense the channel in which signal is transmitted, and they can interfere by jamming the signal. This can prevent the communication between base station and the smart mines. We propose a MAC layer security by adopting frequency hopping for communication with a pre-defined algorithm for random number generation. For implementing frequency hopping, the time synchronization need to be done between the neighboring nodes. Computational complexity of frequency hopping is much less than the TinyECC. Moreover, it provides a MAC level security rather than an application level security.

In this paper, we also propose the use of mobile nodes [3] for wireless charging (inductive recharging) of the static sensor nodes as required. The inductive recharging uses an electromagnetic field to transfer energy between two nodes. Many literatures propose the use of inductive charging to enhance the life of WSN.

III. PROPOSED APPROACH

In this paper, we propose a simple-charging technique using a mobile node to charge the static nodes (smart mines) deployed. For long term deployment, static nodes are either programmed with energy efficient algorithms or equipped with energy harvesting modules. The latter solution is not feasible w.r.t the deployment proposed in [] as the node is buried under the ground. We propose the use of mobile energy bank, which can explore the sensor field, recharge the smart mines and then return back to the base station. If the position of sensor nodes is known in advance, a proper path planning can be done to direct the mobile node for recharging purposes. Since the application environment is hostile and due to geographical phenomena, some of the static nodes deployed will die over time (due to hardware failure) or may get physically displaced. In such scenario a proper path planning is not feasible as the environment is un-known. In such cases, for node recharging, static nodes can adopt any area exploration technique. In real time applications, the recharging should be done with no time delay so that the nodes could resume its function as usual. Area exploration techniques are generally used to cover the region where the static smart mines are deployed so that it will cover all the nodes in minimum amount of time [3].

Multiple mobile nodes based exploration are faster than single mobile node based exploration since it provides better reliability, efficiency and flexibility. The use of multiple mobile nodes can explore an unknown area more quickly and parallel. There are several techniques available for area exploration which includes frontier-based approach[7], market-driven approach [5] and role-based approach [6]. In frontier-based approach, mobile nodes are moved towards the boundary between the discovered and unknown area. In market-driven exploration, mobile nodes place bids on submission, based on traveling cost and expected information gain. Role-based model on the other hand, categorizes mobile nodes into explorer nodes and relay nodes so as to establish a multi hop communication with the base station. The explorers will explore the farthest reaches of their environment and communicate their findings periodically to a common point where they pass their knowledge to a relay station (node). The relays will then act as a link between the explorer nodes and the command center (base station). The relays will communicate the explorer's findings back to the base station.

In this paper, we are proposing the use of the inductive recharging technique, for battery recharging of the smart mines in case of depletion of power using role-based exploration technique. The inductive recharging uses an electromagnetic field to transfer energy between two sensor nodes. We propose a role based exploration approach which provides better reliability than the other approaches. This can be done in a scheduled manner or based on threshold w.r.t the total energy of the network. The total energy of the network can be calculated using the battery monitoring function like the one implemented in the paper[2]. During the exploration, the mobile node approaches each static node and does recharging.

The inductive recharging is done by sending the energy through an inductive coupling to an electrical device, which can then use that energy to charge the batteries or run the device. The chargers use an induction coil which creates alternating electromagnetic fields from within a charging base station. The second induction coil in the static node will take the power from the electromagnetic field and converts it back into electrical current to charge the battery. The two induction coils combine to form an electrical transformer.

As explained in the section 2, approach proposed in [2] is prone to jamming attack. In this paper we propose the use of frequency hopping as MAC level protocol which can be used against jamming attack. In Frequency Hopping (FH), a radio signal communication is done between two or more nodes, by rapidly changing the radio channels following a predetermined pseudo random channel sequence known to both the sender and the receiver. The transmitter sends a request via a predefined frequency channel (control channel). The sender and the transmitter uses a common seed as one of the inputs in a random number algorithm, which then calculates the channel sequence, i.e. the sequence of frequencies that is used for communication. The communication starts at the same point in time, and both the transmitter and the receiver change their frequencies according to the channel sequence. For implementing, the nodes need to be time synchronized. Time synchronization is used to synchronize the time between the base station and the smart mines. Most of the time synchronization schemes for sensor network have 4 basic packet delay components- send time, access time, propagation time and receive time. The best protocol used for time synchronization is the Time synchronization protocol sensor networks.(TPSN). TPSN is a sender-receiver synchronization approach, where the sender initiates and synchronizes its clock with the receiver.

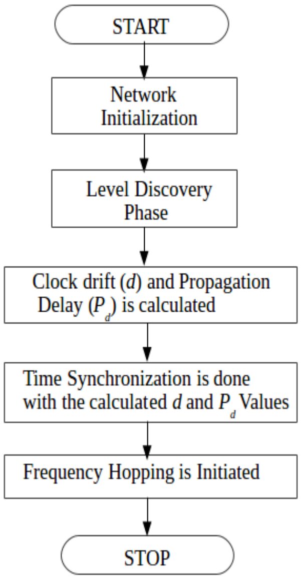
START
Network Initialization
Level Discovery Phase
Clock drift (d) and Propagation Delay (P_d) is calculated
Time Synchronization is done with the calculated d and P_d Values
Frequency Hopping is Initiated
STOP

Fig1 : Time synchronization

Figure 1 shows the flow diagram of TPSN before transmitting data using FH. Once the nodes are deployed, network initialization phase starts where a routing path need to be calculated from every nodes to the base station. When a node is deployed, the parameters such as *node-id*, *location* and the *seed value* are hard-coded. *Node-id* indicate the address of the node, *location* indicate the geographical location while *seed* is a variable used to generate the pseudo-random sequence. It should be noted that each node will be having a different seed value. Routing algorithm explained in [2] is not feasible as the deployment is unstructured. To find a path we propose to use a simple routing protocol like AODV [8]. During the network initialization phase, nodes also learn about their neighboring node and the seed value associated with each neighboring node. This information will be stored in a table for future processing.

TPSN is a sender-receiver synchronization approach [3] where the sender initiates the synchronization and synchronizes its clock to the receiver. The synchronization is achieved in 2 phases:

- Level Discovery Phase
- Clock Synchronization Phase

The level discovery phase is done by making a spanning tree of the whole network and each node is assigned a level. The root of the tree is assumed to be the base station and it will be at level 0. The nodes at level n will be capable of communicating with nodes at level n-1.

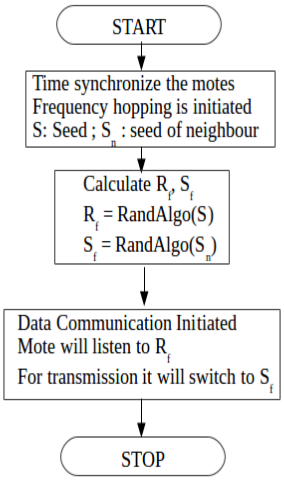
START
Time synchronize the motes
Frequency hopping is initiated
S: Seed ; S_n : seed of neighbour
Calculate R_f, S_f
R_f = RandAlgo(S)
S_f = RandAlgo(S_n)
Data Communication Initiated
Mote will listen to R_f
For transmission it will switch to S_f
STOP

Fig2 : Frequency Hopping

The synchronization phase starts with the child node and each child node is synchronized with its parent node and the process continues up to the root level(base station). Between each sender and the receiver the sender node will send a synchronization request packet to the receiver node at time T1. The receiver node will receive the packet at time T2 and sends an acknowledgement at time T3. The acknowledgement packet contains information about T2 and T3. The sender node will receive this acknowledgment packet at time T4. The sender node will use these four time values to calculate the clock drift(d) and propagation delay (P_d). This synchronization starts at the base station, which will broadcast a time-sync packet to all the smart mines. Once the synchronization between all the smart mines and the base station are achieved, then frequency hopping based can be initialized for data communication.

Figure 2 shows the flow-diagram of frequency hopping. In frequency hopping, we assume that the nodes are already time-synchronized and a local table maintained in each node contain its immediate neighbor information along with its seed value. For data communication, each node needs to calculate the receiving channel (for receiving packets) and the transmission channel (for transmitting packets). As shown in the Figure 3, node n_1 whose seed is s_1 will calculate the receiving channel (R_f) using the function R_f = RandAlgo(s_1), where RandAlgo is the algorithm for pseudo-random number generation. If the node n_1 want to transmit data to node $n_{2,}$ then it calculate the sending channel (S_f) using the function S_f = RandAlgo(s_2), Similarly if the node n_1 want to communicate to node n_3, it calculate the channel at which node n_3 listen to using the pseudo-random algorithm w.r.t the current time and then start its communication. Once the data communication starts, TPSN guarantees that the channel switching is synchronized. Single transceiver in sensor node allows half-duplex communication. This means the nodes can either receive or send data at a time. In case of a node n_1 receiving data from node n_0 and relaying it to n_2, it listen to the channel calculated using the seed value S_1, and switch to the channel (calculated using the seed value S_2) for transferring the data and then switches back to the listening mode. Since the frequency hopping done over time based on the random sequence generated, it will be difficult for an intruder to listen to a particular channel to sniff the data. More over the frequency hopping allow less interference and hence data rate will increase.

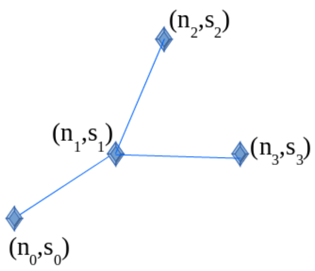

Fig 3: Node to node communication Scenario

The FH pattern generated should appear a truly random number in order for it to ensure the properties of secretiveness and unpredictability. Other secondary properties include a large period, a uniform distribution over all frequency channels so that all the channels are used for maximum efficiency and the seed for the hopping pattern should be a multilevel number with a large linear span. If the period is large enough, then it is very difficult for a jammer to intercept and store the pattern.

An implementation of such MAC level protocol improves security by preventing signal jamming as well as reduces interference. In case of WSN using zigbee protocol, the sixteen orthogonal channels are available, which can be used for Frequency hopping.

IV. IMPLEMENTATION AND CONCLUSION

The implementation of smart mines with inductive charging facility will enhance the life time of the network. Section 2 propose the use of role-based exploration model. A simple C-language based simulation is done to study the performance of role-based exploration. The security architecture proposed in [2] only ensures security at the application level.i.e, between the message transferred between the base station and the smart mine. This paper ensures the security at the MAC level by implementing frequency hopping. Due to limited resources analysis of proposed approach is left for future implementation. Future enhancement consist of using, frontier based approach with long range communication modules for recharging static nodes with the help of mobile nodes.

The paper proposes the use of smart mobile nodes which uses area exploration strategy to charge individual smart mines deployed in an area. It also proposes to secure the physical layer communication between individual smart mines and the base station by implementing the frequency hopping technique by time synchronizing the smart mines and the base station. This will provide a highly reliable, secure smart mines deployed in the area of interest to automate the process of demining. The paper has only given proposals for the implementation.

REFERENCES

[1]. D. G. Jennifer Yick, Biswanath Mukherjee, “Wireless sensor network survey,” Computer Networks, vol. 52, no. 12, pp. 2292 – 2330, 2008.

[2]. Seth, Bharat Udai, and Krishna M. Sivalingam. "Wireless sensor node based smart mine design." Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference on. IEEE, 2012.

[3]. D. Massaguer, C.-L. Fok, N. Venkatasubramanian, G.-C. Roman, and C. Lu, “Exploring sensor networks using mobile agents,” in Proceedings of the fifth international joint conference on Autonomous agents and multiagent systems, pp. 323–325, ACM, 2006

[4]. U. Javed, "Frequency hopping in wireless sensor networks, " M.Sc. Thesis, Helsinki University of Technology., March 2009.

[5]. M. Dias, R. Zlot, N. Kalra, and A. Stentz, “Market-based multirobot coordination: A survey and analysis,” Proceedings of the IEEE, vol. 94, pp. 1257–1270, July 2006

[6]. J. de Hoog, S. Cameron, and A. Visser, “Role-based autonomous multi-robot exploration,” in Future Computing, Service Computation, Cognitive, Adaptive, Content, Patterns, 2009. COMPUTATIONWORLD ’09. Computation World:, pp. 482–487, Nov 2009.

[7]. W. Burgard, M. Moors, C. Stachniss, and F. E. Schneider, “Coordinated multi-robot exploration,” Robotics, IEEE Transactions on, vol. 21, no. 3, pp. 376–386, 2005.

[8]. I. D. Chakeres and E. M. Belding-Royer, “Aodv routing protocol implementation design,” in Distributed Computing Systems Workshops, 2004. Proceedings. 24th International Conference on, pp. 698–703, IEEE, 2004.