Data Gathering Using Sink Mobility with Three Tier Security Scheme in Wireless Sensor Network

S. Aruna
PG Student
SMVEC, Puducherry

Dr. L. M. Varalakshmi
Associate professor
SMVEC, Puducherry

Abstract

Data gathering is a fundamental task of WSN. It aims to collect sensor readings from sensory field at pre-defined sinks (without aggregating at intermediate nodes) for analysis and processing. Research has shown that sensors near a data sink deplete their battery power faster than those far apart due to their heavy overhead of relaying messages. Non-uniform energy consumption causes degraded network performance and shortens network lifetime. Recently, sink mobility has been exploited to reduce and balance energy expenditure among sensors. However, in sensor networks that make use of the existing key pre-distribution schemes for pairwise key establishment and authentication between sensor nodes and mobile sinks, the employment of mobile sinks for data collection elevates a new security challenge. The basic probabilistic and q-composite key pre-distribution schemes, an attacker can easily obtain a large number of keys by capturing a small fraction of nodes, and hence, can gain control of the network by deploying a replicated mobile sink preloaded with some compromised keys. This article describes a three-tier general framework that permits the use of any pairwise key pre-distribution scheme as its basic component and requires two separate key pools, one for the mobile sink to access the network, and one for pairwise key establishment between the sensors. In this paper, we investigate the theoretical aspects of the uneven energy depletion phenomenon around a sink, and address the problem of energy-efficient data gathering by mobile sinks with Three-Tier security.

Keywords-Distributed, security, wireless sensor networks.

1.Introduction

Recent advances in the development of low cost sensing devices and microminiaturization have further advanced the scope of applications of wireless sensor networks (WSNs). WSN based solutions have been designed and implemented in diverse areas, including environment and habitat monitoring, building automation, disaster and waste management, infrastructure monitoring, etc. [1]. Sensor nodes used in these applications are characterized by limited resources in terms of memory, computation power, and energy [2]. In particular, WSNs deployed for remote area monitoring usually comprise a large number of tiny static sensing devices, which are deployed in an ad hoc manner over a geographically wide area to sense parameters of interest. Such a random and uncontrolled deployment results in unknown network topology which, along with dynamic environment, low bandwidth, limited battery power and constrained storage capacity of the nodes, necessitates that each node always knows an energy efficient routing path to the sink with low congestion. In addition to maintaining energy efficient routing paths to the sink two other techniques often used for achieving energy efficiency are sink mobility [3,4] and duty cycling of the nodes [5].

The sink can be static or mobile, and can be placed at different locations in the WSN. In the case of a static sink, nodes located in the vicinity of the sink deplete their energy (and die) much earlier compared to the nodes located farther away from the sink due to higher data relaying load. In order to address this issue, sink mobilization has been introduced, where the sink moves along a certain path through the network. It has also been shown that in most cases sink mobility helps in balancing the routing load and hence energy dissipation of the nodes.

The sensed data often need to be sent back to the base station for analysis. However, when the sensing field is too far from the base station, transmitting the data over long distances using multihop may weaken the security strength (e.g., some intermediate may modify the data passing by, capturing sensor nodes, launching a wormhole attack , a sybil attack , selective forwarding , sinkhole), and increasing the energy consumption at nodes near the base station, reducing the lifetime of the network. Therefore, mobile sinks (MSs) (or mobile soldiers, mobile sensor nodes) are essential components in the operation of many sensor network applications, including data collection in hazardous environments [6], [7], [8], localized reprogramming, oceanographic data collection, and military navigation [9].

In many of these applications, sensor nodes transmit critical information over the network; therefore, security services, such as, authentication and pairwise key establishment between sensor nodes and mobile sinks, are important. However, the resource constraints of the sensors and their nature of communication over a wireless medium make data confidentiality and integrity a non-trivial task. Traditional schemes in ad hoc networks using asymmetric keys are expensive due of their storage and computation cost. These limitations make key pre-distribution schemes [10], [11], [12], [13], [14], [15], [16] the tools of choice to provide low cost, secure communication between sensor nodes and mobile sinks.

During the data collection technique in mobile sink sensor networks, security is an important factor. Node need to be authenticate before start the data collection process. At the same time sensors also need to authenticate the sink. After authentication takes place, start the data communication process with specified rule. During the data collection sensor send their data with encrypting the data packets and send it to the sink node. When sink receive the data it decrypt the packet and check for the adversary modification during data transmission. This node authentication, data encryption and decryption use different cryptography technology. Using three-tier it secures the communication process.

1.1 Mobile Sink Wireless Sensor Networks

In Mobile Sink Wireless Sensor Networks all the sensors are statically deployed to sense the environment and mobile sink traverse the networks. It overcomes the problem of the sink neighbourhood problem. In the sink neighbourhood problem is neighbour nodes of sink participate more in the data transmission. The result is the faster energy deplete compared to other nodes in the network. If we look over the energy conservation model sensor deplete some amount of energy during the data receiving and the data transmission. As the sensor those are close to the sink, participate in more data transmission i.e. for them and for those sensors away from the sink in the same direction.

In MSWSN all nodes are static other than the sink in the network. Mobile sink traverse randomly to collect the sensor data. It may be collect with one hop or multi hop communication and our proposed model is the one hop data collection. As sink traversing throughout the network for data collection so the neighbour of the sink is not fixed, so neighbourhood problem will not arises. Here we use LR-WPAN IEEE 802.15.4 low cost wireless link. IEEE 802.15.4 intends the lower network layers of a type of wireless personal area network (WPAN) which focuses on low cost, low speed global communication between the sensors.

IEEE 802.15.4 security consists of four kinds of security services such as access control, message integrity, message confidentiality, and replay protection. The access control feature should prevent illegal users to participate in the process. In other word, only authorized users can able join in a legitimated network. Message integrity means the validity of transferred data and message authentication implies message sender’s verification using cryptographic function. These message integrity and message authentications are possible using Message Authentication Code (MAC) in IEEE 802.15.4. The MAC is appended to each data packet sent.

A malicious node can participate in the data collection process by showing it as the sink node. Then all the sensed data collected by the malicious node, for that we need to authenticate the node before sending the sensed data. If sensors send its packets without encryption then malicious node can accept the packet then it can modify the content of the packet. So we’ll lose the original content of the data. Data is neither to be modified nor be dropped. We need to keep data freshness. For that we need to use cryptography concept to secure the data collection technique. The security requirements of mobile sink sensor networks and the attacks possible in each layer.

We propose a framework to establish secure energy efficient data collection with mobile sink. So that data can be collected as a secure manner and prolong network lifetime.

2. The three-tier security scheme

In this study, we have chosen the Blundo scheme [19] to construct our approach. As we shall see, the Blundo scheme provides a clear security guarantee. Use of the Blundo scheme, therefore, greatly eases the presentation of our study and enables us to provide a clearer security analysis.

In the proposed scheme, we use two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Polynomials from the mobile polynomial pool are used to establish the authentication between mobile sinks and stationary access nodes, which will enable these mobile sinks to access the sensor network for data gathering. Thus, an attacker would need to compromise at least a single polynomial from the mobile pool to gain access to the network for the sensor's data gathering. Polynomials from the static polynomial pool are used to ascertain the authentication and keys setup between the sensor nodes and stationary access nodes.

Prior to deployment, each mobile sink randomly picks a subset of polynomials from the mobile polynomial pool. In our scheme, to improve the network resilience to mobile sink replication attack as compared to the single polynomial pool-based approach, we intend to minimize the probability of a mobile polynomial being compromised if R_c sensor nodes are captured. As an adversary can use the captured mobile polynomial to launch a mobile sink replication attack, we achieve this by having a small fraction of randomly selected sensor nodes carry a polynomial from the mobile polynomial pool. These preselected sensor nodes are called the stationary access nodes. They act as authentication access points for the network and trigger sensor nodes to transmit their aggregated data to the mobile sinks. A mobile sink sends data request messages to the sensor nodes via a stationary access node. The mobile sink's data request messages will initiate the stationary access node to trigger sensor nodes to transmit their aggregated data to the requested sink. Each stationary access node may share a mobile polynomial with a mobile sink. All sensor nodes, including the stationary access nodes, randomly select a subset of polynomials from the static polynomial pool. The advantage of using separate pools is that mobile sink authentication is independent of the key distribution scheme used to connect the sensor network. We divide our scheme into two stages: static and mobile polynomial *pre-distribution* and key discovery between a mobile sink and a sensor node.

Stage 1 (Static and mobile polynomial pre-distribution). Stage 1 is performed before the nodes are deployed. A mobile polynomial pool M of size |M| and a static polynomial pool S of size |S| are generated along with the polynomial identifiers. All mobile sinks and stationary access nodes are randomly given Km and one polynomial (*K*m > 1) from M. The number of mobile polynomials in every mobile sink is more than the number of mobile polynomials in every stationary access node. This assures that a mobile node shares a common mobile polynomial with a stationary access node with high probability and reduces the number of compromised mobile polynomials when the stationary access nodes are captured. All sensor nodes and the preselected stationary access nodes randomly pick a subset of K_s and K_s — 1 polynomials from *S*. Fig. 1 shows the key discovery between the mobile node and stationary node.

Stage 2 (Key discovery between mobile node and stationary node). To establish a direct pairwise key between sensor node u and mobile sink *v*, a sensor node u needs to find a stationary access node a in its neighbourhood, such that, node a can establish pairwise keys with both mobile sink *v* and sensor node *u*. In other words, a stationary access node needs to establish pairwise keys with both the mobile sink and the sensor node. It has to find a common mobile polynomial with the mobile sink and a common static polynomial with the sensor node. To discover a common mobile/static polynomial, a sensor node *i* may broadcast a list of polynomial IDs, or alternatively, an encryption list, α , $E_{Kv}(\alpha)$, *v* = 1,…, $|K_{si}|$, where K*v* is a potential pairwise key and the other node may have as suggested in [10] and [11]. When a direct secure path is established between nodes *u* and *v*, mobile sink *v* sends the pairwise key K_c to node *a* in a message encrypted and authenticated with the shared pairwise key K_v ;*a* between *v* and *a*. If node a receives the above message and it shares a pairwise key with u, it sends the pairwise key K_c to

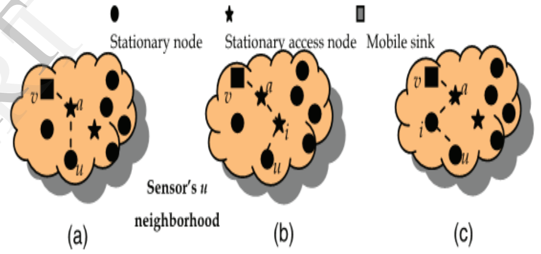

Fig.1. (a) Direct key discovery. (b) Indirect key discovery through intermediate stationary node *i*. (c) Indirect key discovery through intermediate stationary access node *i*.

node *u* in a message encrypted and authenticated with pairwise key $K_a;u$ between *a* and *u*.

If the direct key establishment fails, the mobile sink and the sensor node will have to establish a pairwise key with the help of other sensor nodes. To establish a pairwise key with mobile sink *v*, a sensor node *u* has to find a stationary access node *a* in its neighbourhood such that node *a* can establish a pairwise key with both nodes *u* and *v*. If node *a* establishes a pairwise key with only node *v* and not with *u*. As the probability is high that the access node *a* can discover a common mobile polynomial with node *v*, sensor node *u* needs to find an intermediate sensor node *i* along the path *u* — *i* — *a* — *v*, such that intermediate node *i* can establish a direct pairwise key with node *a*.

3. Energy efficiency by sink mobility

This section briefly discusses how to achieve energy efficiency by exploiting sink mobility. Sink mobility may be classified as uncontrollable or controllable in general. The former is obtained by attaching a sink node on certain mobile entity such as an animal or a shuttle bus, which already exists in the deployment environment and is out of control of the network. The latter is achieved by intentionally adding a mobile entity e.g., a mobile robot or a unmanned aerial vehicle, into the network to carry the sink node. In this case, the mobile entity is an integral part of the network itself and thus can be fully controlled.

3.1 Delay-tolerant scenarios

In delay-tolerant WSN for applications such as habitat monitoring and water quality monitoring, energy usage optimization embraces a lot of options. To maximize energy savings for sensors, direct contact data collection is the best option. That is, sinks visit (possibly at slow speed) all data sources and obtain data directly from them. This method completely eliminates the message relay overhead of sensors, and thus optimizes their energy savings. However, it has large data collection latency for the slow moving sinks. To reduce time delay, sinks may visit only a few selected rendezvous points (RPs) ,where sensor readings of all data sources are buffered and possibly aggregated, avoiding long travel distance at energy cost of multi-hop data communication. Both direct contact data collection and rendezvous based data collection can be supported by uncontrollable or controllable sink mobility. Fig 2.1(a) depicts taxonomy of existing approaches for energy-efficient data collection by mobile sinks in delay-tolerant WSN. At the top level of the taxonomy are the two classes of collection methods, i.e., direct-contact and rendezvous-based. Each is further divided into three sub-classes according to their employed techniques.

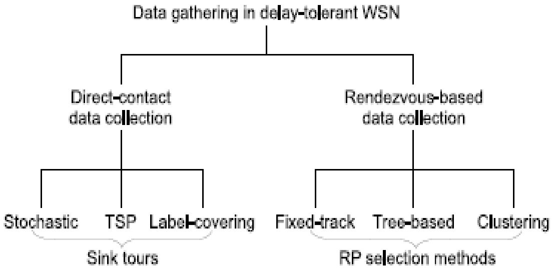
Data gathering in delay-tolerant WSN
Direct-contact data collection
Rendezvous-based data collection
Stochastic
TSP
Label-covering
Fixed-track
Tree-based
Clustering
Sink tours
RP selection methods

Fig.2.1(a) Delay-tolerance WSN

3.2 Real-time scenarios

In real-time WSN for applications like battle field surveillance and forest fire detection, sensor readings ought to be timely collected by sinks. With effective mobile-sink-based data dissemination (i.e., source-to-sink routing) methods, network lifetime can be prolonged by adaptively relocating sink nodes to positions with largest energy gain as the network evolves.

For example, Banerjee et al. suggested that sinks move toward data sources, or energy-intense areas, or the combination thereof; Luo and Hubaux concluded optimal sink mobility strategy is to move along the periphery of the network when the network has a circular shape and shortest path routing is used. Intelligent sink relocation requires controllable sink mobility. Uncontrollable (e.g., random or fixed-track) sink movement may also balance energy consumption since the role of “hot spot” rotates among sensors. But, it has relatively inferior performance.

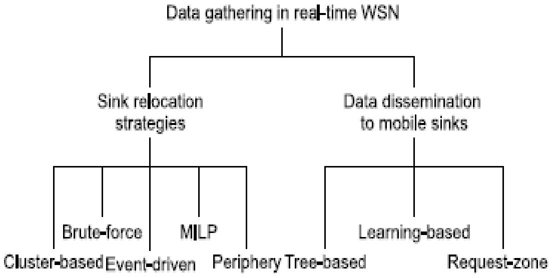
Data gathering in real-time WSN
Sink relocation strategies
Data dissemination to mobile sinks
Brute-force
MILP
Learning-based
Cluster-based
Event-driven
Periphery
Tree-based
Request-zone

Fig.2.2 (b) Real-time WSN

Figure 2.2(b) shows taxonomy of existing approaches for energy-efficient data gathering in real-time WSN. At the top level of the taxonomy are the two research sub-problems, i.e., sink relocation and data dissemination, each followed by representative solutions at the lowest level.

4. Sink mobility in delay-tolerant networks

In this section, we review the literature on energy-efficient data collection by mobile sinks in delay-tolerant WSN. We examine direct-contact data collection methods first.

4.1 Direct-contact data collection

In direct-contact data collection, a mobile sink collects data directly from data sources by one-hop communication. Sink may retransmit data or, if needed, physically carry the data to a fixed base station. This approach minimizes energy consumption among sensors for communication since sensors do not need to forward messages for each other. In this scenario, the main concern is the computation of the best sink trajectory that covers all data sources and minimizes data collection delay.

4.2 Stochastic data collection trajectory

Shah et al. considered stochastic sink mobility and proposed a simple data collection algorithm. In their proposal, sensors buffered their measurements locally and wait for the arrival of a mobile sink. Multi-sink scenario is also considered. Each sink moves randomly and collects data from encountered sensors in its communication range. Collected data are then carried by the sink to a wireless access point (e.g., a fixed base station).

In the case of stochastic sink mobility, energy consumption at sensor side is only due to sink discovery and subsequent data transfer. Assume each sink broadcasts a beacon message while moving. A straightforward way of sink discovery is to monitor the wireless communication channel. Whenever a sensor hears the beacon message it concludes that a sink arrives. However, constant channel monitoring is very expensive in energy. Chakrabarti et al. show that, if sinks (e.g., mounted on shuttle buses) move along regular path, then sensors can predict their arrival after being allowed a learning curve for their movement pattern.

After discovering a sink, data transfer should also start in an intelligent way. If a sensor simply transmits as soon as it discovers the sink, data may not be successfully delivered or may be delivered with many retrials, wasting energy. According to [ACG+06](G. Anastasi, M. Conti, E. Gregori, C. Spagoni, and G. Valente.), message loss probability drops with decreased sensor-sink distance. Suppose the sink passes by sensors along straight line. To minimize energy consumption, data transfer should take place in the time interval with minimum message loss probability, which is exactly around the minimum sensor-sink distance point. From this consideration, Anastasi et al. proposed an adaptive data transfer protocol. In that, the contact time $\hat{f}(n+1)$ for the $(n+1)$-st passage is estimated by function $\hat{f}(n+1) = \alpha\, f(n) + (1 - \alpha)\, \hat{f}(n)$, where $f(n)$ and $\alpha(0 < \alpha < 1)$ represent the time elapsed since the previous (the n-th passage) contact, the duration of contact, or the time between contact and data transfer, or other relevant measure (different measure has different function and its parameter). According to the estimation, sensors start data transfer properly in time and transmit a pre-defined number of bits. If contact time is large enough for sensors to perform a sleep-wakeup circle before transmitting, they will do so to save energy.

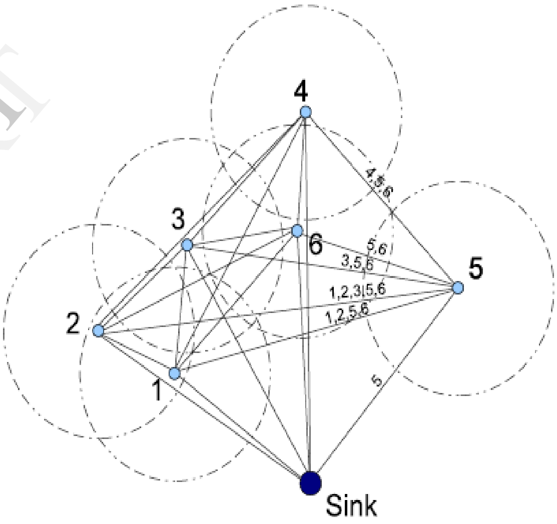

Fig.3. Complete graph of sensors and the sink node

5. Proposed data collection method

We consider there are n numbers of static homogenous sensor nodes placed uniformly in a square region given by a geographical area, for sensing data or monitoring events. Single mobile sink travels in the squared monitored region to collect data by one hop communication. It follows the proposed mobility model to travel through the service area to collect data. Sink collects the data from the sensors; those are within the radio range of the sink. It follows one hop data collection process. Data collection takes place in three step process. There are two types of data collection; one is proactive data collection and another is reactive data collections. In proactive data collection method sensed data distributed and store throughout the network for later retrieval of sink. In reactive data collection method data send to the sink after detection of sinks presence or query. Our model follows the reactive data collection. Fig 4 shows the sequence diagram of data collection.

During one hop data collection it performs with three step process, as shown in the sequence diagram. We need to specify the initial position of the sink. After that sink movement is based upon the proposed mixed mobility model. With following this mobility model sink changes its position and each new position it performs data collection operation with three step process. In first step, sink broadcast a new beacon frame to alert the sensors within its range for sink's presence. In second step, after proper identifying the sink node sensors send their sensed data to the sink. In last step, before sink changes position it broadcast a new beacon frame to alert the sensors within its range to stop the data transmission. We follow the last step to reduce the packet drop.

In Algorithm 1 initially sink starts motion from the initial position of the bounded services area. Sink changes its relative position according to the proposed mobility. Sink broadcasts a start beacon frame to the neighbour nodes.

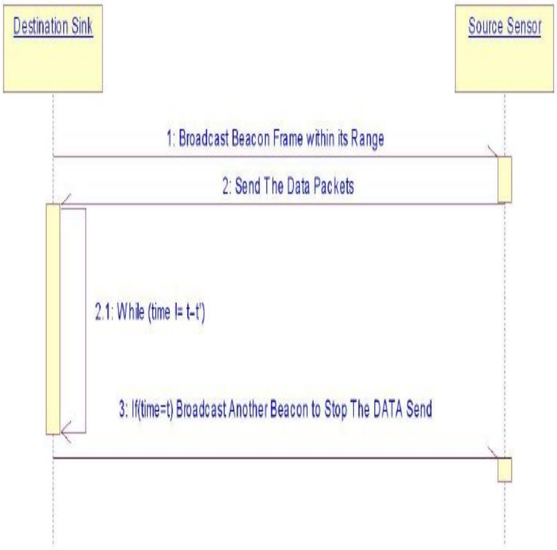
Destination Sink
Source Sensor
1: Broadcast Beacon Frame within its Range
2: Send The Data Packets
2.1: While (time != t-t')
3: If(time=t) Broadcast Another Beacon to Stop The DATA Send

Fig.4. Sequence diagram of communication between sensor and sink.

After receiving the beacon frame each sensor node set their value and starts to send the data packets to the sink till receives the stop beacon frame. Just before sink changes its position *(T−δT)* time sink broadcasts another beacon frame to reset the neighbour nodes and stop the transmission, to reduce the packet drop. After that sink changes to a new position and follow the same procedure every time.

Algorithm 1

t= Current time

T= Simulation time //End time of the program

τ= Pause time //Remain same throughout the program

p(x, y) = Position of the sink

b_cast(id, start/stop) = Beacon frame broadcast by the sink.

```
initial position sink = p(x,y)
z←τ
t←0
repeat
    Sink= b cast(id, start)
    while (t ≤ z−δτ) do
        Sink= recv data(packets)
    end while
    if (t ≥ z−δτ) then
        Sink= b cast(id,stop)
    end if
    new position sink = p(x′,y′)
    z←t+τ
until ( t = T )
```

6. Simulation analysis

In this section we evaluate the performance of the proposed model and compare it with the existing technology with static network. The experiment has been done in ns 2.34, we have taken 100 random sensor nodes in the 1000x1000 meter area. Initially all sensor nodes have same level of enegy, i.e., 1 joule and the communication range 25 meters. The transmitting and receiving energy is 50 nJpb and transmit amplifier to achieve an acceptable form is 100pJpb.

Here we compared our proposed model Mobile Sink Wireless Sensor Networks (MSWSN) with traditional protocol flooding and flat routing protocol Sensor Protocol for Information via Negotiation (SPIN). SPIN is a negotiation base multi cast routing protocol. Source first negotiates among the neighbours before start the data transfer.

Communication overhead becomes main issue in this type of network, which tends to MAC sub layer. Sensors transmit the packets to the sink node and sink collect it with DSR protocol in our simulation model.

In this Fig. 4 we have shown the delivery ratio of three routing protocols. Initially in flooding delivery ratio is higher than the SPIN because of their redundant data delivery nature. As soon as node dies, delivery ratio decreases. In SPIN the difference of minimum and maximum delivery ratio is less as compared to flooding. In the proposed model delivery ratio is nearly 100

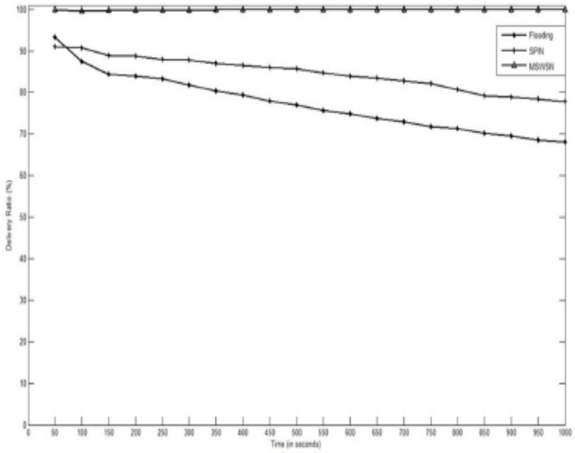

Fig.4. Delivery ratio vs Time

7. Conclusion

This paper, a new framework for energy efficient secure data collection is proposed. The proposed framework uses a new approach of one hop communication and node authentication on the base of secure energy efficient algorithms for sensor networks. We have simulated the proposed model and compared with traditional protocol for mobile sensor networks. Here we use symmetric key distribution for secure data collection. Communication between sensor nodes and the sink is secured as the sensor data is encrypted using symmetric key. In the proposed scheme the large prime is generated in a fixed time interval of time to avoid replay attack and keep data freshness by strengthening the authentication mechanism.

8. References

[1] C.S. Raghavendra, K.M. Sivalingam, T. Znati, Wireless Sensor Networks, Kluwer Academic Publishers, 2004.

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Communications Magazine 40 (2002) 102–114.

[3] J. Luo, J. Panchard, M. Piorkowski, M. Grossglauser, J.-P. Hubaux, Mobiroute: routing towards a mobile sink for improving lifetime in sensor networks, in:Proceedings of IEEE International Conference on Distributed Computing in Sensor Networks (DCOSS), 2006, pp. 480–497.

[4] F. Ye, H. Luo, J. Cheng, S. Lu, L. Zhang, A two-tier data dissemination model for large-scale wireless sensor networks, in: Proceedings of 8th Annual international Conference on Mobile Computing and Networking, MobiCom ‘02, Atlanta, Georgia, USA, September 23–28, 2002, pp. 148–159.

[5] L. Wang, Y. Xiao, A survey of energy-efficient scheduling mechanisms in sensor networks, Mobile Network Applications 11 (2006) 723–740.

[6] A. Kansal, A. Somasundara, D. Jea, M. Srivastava, and D. Estrin, “Intelligent Fluid Infrastructure for Embedded Networks,” Proc. Second ACM Int’l Conf. Mobile Systems, Applications, and Services (MobiSys ’04), June 2004.

[7] Y. Tirta, Z. Li, Y. Lu, and S. Bagchi, “Efficient Collection of Sensor Data in Remote Fields Using Mobile Collectors,” Proc. 13th Int’l Conf. Computer Comm. and Networks (ICCCN ’04), Oct. 2004.

[8] A. Rasheed and R. Mahapatra, “An Energy-Efficient Hybrid Data Collection Scheme in Wireless Sensor Networks,” Proc. Third Int’l Conf. Intelligent Sensors, Sensor Networks and Information Processing, 2007.

[9] W. Zhang, G. Cao, and T. La Porta, “Data Dissemination with Ring-Based Index for Wireless Sensor Networks,” Proc. IEEE Int’l Conf. Network Protocols (ICNP), pp. 305-314, Nov. 2003.

[10] L. Eschenauer and V.D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks,” Proc. ACM Conf. Computer Comm. Security (CCS ’02), pp. 41-47, 2002.

[11] H. Chan, A. Perrig, and D. Song, “Random Key Pre-Distribution Schemes for Sensor Networks,” Proc. IEEE Symp. Research in Security and Privacy, 2003.

[12] D. Liu, P. Ning, and R.Li. Establishing, “Pairwise Keys in Distributed Sensor Networks,” Proc. 10th ACM Conf. Computers and Comm. Security (CCS ’03), pp. 52-61, Oct. 2003.

[13] H. Chan, A. Perrig, and D. Song, “Key Distribution Techniques for Sensor Networks,” Wireless Sensor Networks, pp. 277-303, Kluwer Academic, 2004.

[14] D. Liu and P. Ning, “Location-Based Pairwise Key Establishments for Static Sensor Networks,” Proc. First ACM Workshop Security Ad Hoc and Sensor Networks, 2003.

[15] S. Zhu, S. Setia, and S. Jajodia, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,” Proc. 10th ACM Conf. Computers and Comm. Security (CCS ’03), pp. 62-72, Oct. 2003.

[16] A. Rasheed and R. Mahapatra, “An Efficient Key Distribution Scheme for Establishing Pairwise Keys with a Mobile Sink in Distributed Sensor Networks,” Proc. IEEE 27th Int’l Performance Computing and Comm. Conf. (IPCCC ’08), pp. 264-270, Dec. 2008.