Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.1139 – 1148

RESEARCH ARTICLE

A New Approach for Key Forwarding Scheme in WSN Using Mobile Sink

E.Revathi[1], C.Darwin[2], G.Vivitha[3]
[1](Assistant Professor, Department of Computer Science and Engineering)
[3](PG Scholar, Department of Computer Science and Engineering)
[1,3](P.S.R.Rengasamy College of Engineering for Women, Sivakasi, Tamil Nadu, India)
[1](E-mail: e.revathisri@gmail.com), [3](E-mail:vivithasri86@gmail.com)
[2](Assistant Lecturer in Information System Networking Engineering, St. Joseph university, Tanzania)
[2](E-mail:cdarwin2006@gmail.com)

Abstract-A dynamic en-route filtering scheme is to address both false report injection attacks and DoS attacks in wireless sensor networks. In our scheme, sensor nodes are organized into clusters. Each legitimate report should be validated by multiple message authentication codes (MAC), which are produced by sensing nodes using their own authentication keys. The authentication keys of each node are created from a hash chain. Before sending reports, nodes disseminate their keys to forwarding nodes using Hill Climbing approach. Then, they send reports in rounds. In each round, every sensing node endorses its reports using a new key and then discloses the key to forwarding nodes. Using the disseminated and disclosed keys, the forwarding nodes can validate the reports. Each node can monitor its neighbors by overhearing their broadcast, which prevents the compromised nodes from changing the reports. Report forwarding and key disclosure are repeatedly executed by each forwarding node at every hop; until the reports are dropped or delivered to the base station. We assume that the topologies of wireless sensor networks change frequently either because sensor nodes are prone to failures or because they need to switch their states between Active and Sleeping for saving energy. This paper also proposes a framework to maximize the life time of WSN by using mobile sink. Each node does not need to send the data immediately as it becomes available. Instead the node can store the data temporarily and transmit it when the mobile sink is at the most favorable location for achieving the longest WSN lifetime.

Index Terms-- Data reporting, Delay-tolerant applications, En-route filtering scheme, Lifetime maximization, Mobile sink, Wireless Sensor network

I. INTRODUCTION

Wireless Sensor Network (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance and is now used in many industrial and civilian application areas, including industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control. Each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source, usually a battery. A sensor node might vary in size, cost of sensor nodes is similarly variable, depending on the size of the sensor network and the complexity required of individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and bandwidth.

In wireless sensor networks, adversaries can inject false data reports via compromised nodes and launch Denial of service attacks against legitimate reports. Recently, a number of filtering schemes against false reports have been proposed which is shown in figure 1 wireless sensor network architecture.

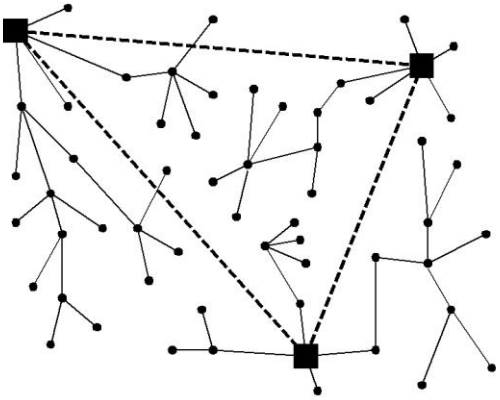

Figure 1: Wireless Sensor Network Architecture

However, they either lack strong filtering capacity or cannot support highly dynamic sensor networks very well. Moreover, few of them can deal with DoS attacks simultaneously. In this paper, we propose a dynamic en-route filtering scheme that addresses both false report injection and DoS attacks in wireless sensor networks. In our scheme figure 2, each node has a hash chain of secrete keys used to send files; meanwhile, a file should be secured by a certain number of nodes. First, each node send its key to forwarding nodes. Then, after sending reports, the sending nodes disclose their keys, allowing the forwarding nodes to verify their reports[1]. We design the Hill Climbing key dissemination approach that ensures the nodes closer to data sources have stronger filtering capacity. Moreover, we exploit the broadcast property of wireless communication to defeat Denial of service attacks and adopt multipath routing to deal with the topology changes of sensor networks. Simulation results show that compared to existing solutions, our scheme can drop false reports earlier with a lower memory requirement, especially in highly dynamic sensor networks. This paper proposes a framework to maximize the lifetime of the wireless sensor networks (WSNs) by using a mobile sink when the underlying applications tolerate delayed information delivery to the sink. Within a prescribed delay tolerance level, each node does not need to send the data immediately as it becomes available. Instead, the node can store the data temporarily and transmit it when the mobile sink is at the most favorable location for achieving the longest WSN lifetime. To find the best solution within the proposed framework, we formulate optimization problems that maximize the lifetime of the WSN subject to the delay bound constraints, node energy constraints, and flow conservation constraints. We conduct extensive computational experiments on the optimization problems and find that the lifetime can be increased significantly as compared to not only the stationary sink model but also more traditional mobile sink models. We also show that the delay tolerance level does not affect the maximum lifetime of the WSN. Although the lifetime of a WSN can be defined in many ways, we adopt the widely used definition, which is the time until the first node exhausts its energy. Communication in a WSN often has the many-to-one property in that data from a large number of sensor nodes needs to be concentrated to one or a few sinks. Since multihop routing is generally needed for distant sensor nodes to send data to the sink, the nodes near the sink can be burdened with relaying a large amount of traffic from other nodes. This phenomenon is sometimes called the “crowded center effect” or the “energy hole problem”[5]. However, by moving the sink in the sensor field, one can avoid or mitigate the energy hole problem and expect an increased network lifetime. Through performance analysis our scheme is efficient with respect to the security it provides, and it allows a tradeoff between security and performance. The key management framework assures both node to sink and node to node authentication along report forwarding routes. It is an Energy efficient Dynamic key management scheme which performs localized rekeying to minimize overhead. Due to advancement of sensor technology WSN can consist of large number of low cost, low power and small sensor nodes.

1.0 System Architecture

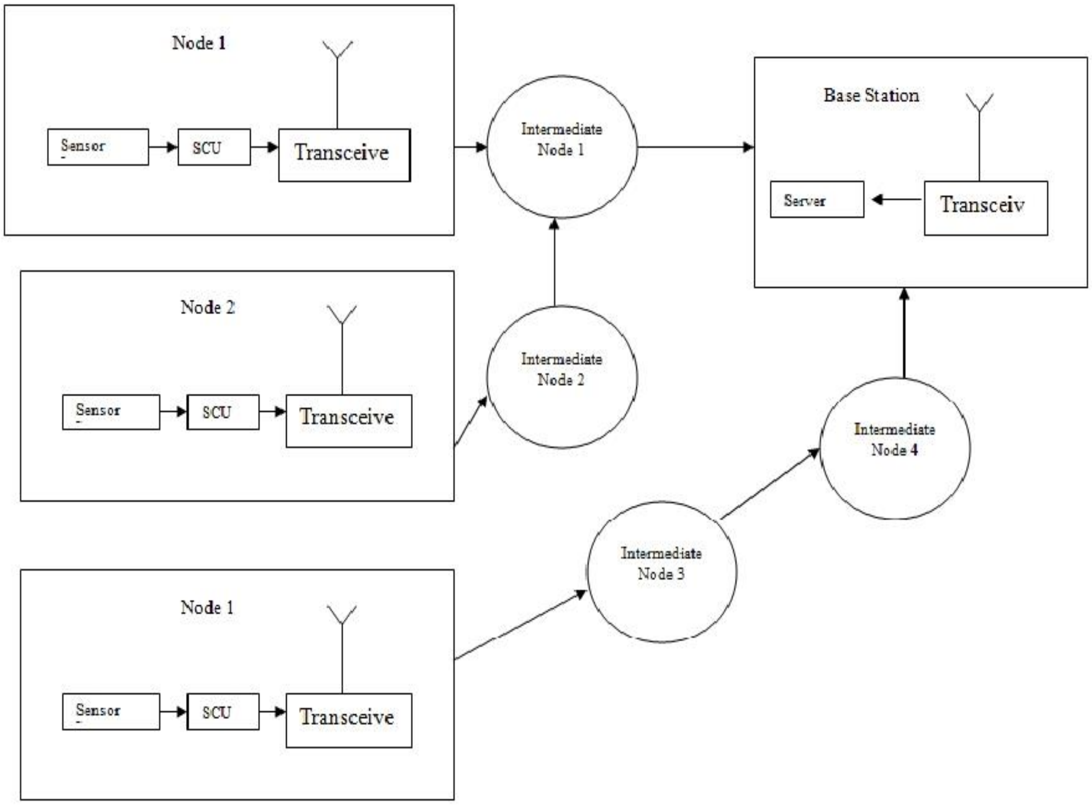

Figure- 2: Connection between Sensor Nodes

A compromised node injects false reports in various locations. Large quantities of such bogus reports cause false alarms. Considerable amount of energy and bandwidth could be wasted in delivering false reports. The user may also be overwhelmed and miss a real event is shown in figure 3. We present a scheme for addressing this form of attack, which we call a false data injection attack. Our scheme enables the base station to verify the authenticity of a report that it has received as long as the number of compromised sensor nodes does not exceed a certain threshold. Further, our scheme attempts to filter out false data packets injected into the network by compromised nodes before they reach the base station, thus saving the energy for relaying them. Each Network will consist of number of sensor nodes connected to the server which acts a receiver part of all the sensor nodes. Communication is done via wireless medium. Here in the flow diagram figure 4 we consider three nodes, first will be sender and second will be intermediate node and third will be receiver. Data acquired will be encrypted using a dynamic key and transmitted to the intermediate node where the data is retrieved and again encrypted with new key. This will be received by the receiver module in a secure way. Next Multipath routing is established for Throughput maximization by which data generated from same node is multiplied to different copied and routed via different paths. Our performance analysis shows this scheme is efficient with respect to the security it provides and allows a tradeoff between security and performance. Therefore there is a need to use dynamic key management scheme that can change the administrative keys by period and on demand or upon detection of node capture. This scheme enhances the network survivability. The major concern of dynamic keying is a designing the rekeying mechanism. When the compromised nodes are detected, the infected clusters can be easily quarantined by the base station.

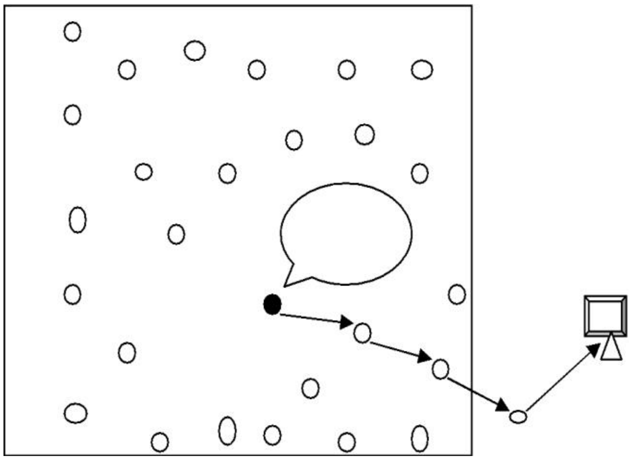

Figure: 3 Compromised Node injecting False Report

A compromised node injects false reports of non-existent tanks “appearing” in various locations. Large quantities of such bogus reports cause false alarms. Considerable amount of energy and bandwidth could be wasted in delivering false reports. The user may also be overwhelmed and miss a real event. A few recent research efforts [3] have proposed mechanisms to provide node and message authentication for sensor networks to prevent false report injection by an outside attacker. However these proposed security mechanisms are rendered ineffective when any single node is compromised. In a large-scale sensor network, detecting and purging bogus reports injected by compromised nodes is a great research challenge. Once a node is compromised, all the security information stored in that node becomes accessible to the attacker. The compromised node can successfully authenticate bogus reports to a neighbor, which has no way to differentiate such false reports from legitimate ones. Although in theory one could apply public-key based authentication mechanism to sensor networks and revoke the key of any compromised node, in reality the computation and storage constraints of small sensor nodes make mechanisms based on asymmetric cryptography. Node and message authentications [3] prevent naive impersonation of a sensor node, however they cannot block the injection of false sensing reports by compromised sensor nodes. We present a dynamic En-route Filtering (DEF) mechanism that can detect and drop such false reports. DEF requires that each sensing report be validated by multiple keyed message authentication codes , 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 Message authentication code probabilistically and drops those with invalid Message authentication code at earliest points. The sink further filters out remaining false reports that escape the en-route filtering. When a sensing target occurs in the field, multiple surrounding sensors collectively generate a legitimate report that carries multiple message authentication codes.

II. SYSTEM STUDY

2.0 Existing System

In the present system, through exploiting the static and location aware nature of WSNs, we came up with a location-aware end-to-end security framework to address the vulnerabilities in existing security designs. In our design, the secret keys are bound to geographic locations, and each node stores a few keys based on its own location[2]. This location-aware property successfully limits the impact of compromised nodes only to their vicinity without affecting end-to-end data security. Furthermore, the proposed multifunctional key management framework assures both node-to-sink and node-to-node authentication along report forwarding routes.

2.1 Disadvantages of Existing System

LEDS utilize location-based keys to filter false reports. It assumes that sensor nodes can determine their locations in a short period of time. However, this is not practical, because many localization approaches take quite long and are also vulnerable to malicious attacks. LEDS tries to address selective forwarding attacks by allowing a whole cell of nodes to forward one report; however, this incurs high communication overhead.

2.2 Proposed System

In this new System, we propose a dynamic en-route filtering scheme to address both false report injection attacks and Denial of service attacks in wireless sensor networks. In our scheme, sensor nodes are organized into clusters. Each legitimate report should be validated by multiple message authentication codes, which are produced by sensing nodes using their own authentication keys. The authentication keys of each node are created from a hash chain. Before sending reports, nodes disseminate their keys to forwarding nodes using Hill Climbing approach. Then, they send reports in rounds. In each round, every sensing node endorses its reports using a new key and then discloses the key to forwarding nodes. Using the disseminated and disclosed keys, the forwarding nodes can validate the reports.

2.3 Advantages of Proposed System

It can offer stronger filtering capacity and drop false reports earlier with an acceptable memory requirement, where the filtering capacity is defined as the average number of hops that a false report can travel. It can address or mitigate the impact of DoS attacks such as report disruption attacks and selective forwarding attacks. It can accommodate highly dynamic sensor networks and should not issue the process of path establishment or reparation frequently. It should not rely on any fixed paths between the base station and cluster-heads to transmit messages[3]. It should prevent the uncompromised nodes from being impersonated.

III. PROBLEM STATEMENT

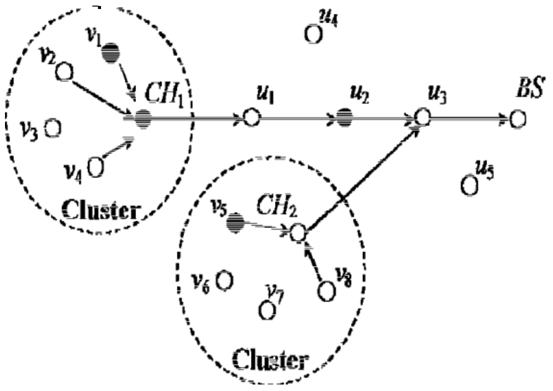

Figure 4: Sensor nodes organized into clusters.

From figure 4 the big dashed circles outline the regions of clusters.CH and BS denote Cluster-Head and Base Station respectively.u1 to u4 are forwarding nodes, and v1 to v8 are sensing nodes (they can also serve as forwarding nodes for other clusters). The black dots represent the compromised nodes, which are located either within the clusters or en-route.

3.0 Goals

1) It can offer stronger filtering capacity and drop false reports earlier with an acceptable memory requirement, where the filtering capacity is defined as the average number of hops that a false report can travel.
2) It can address or mitigate the impact of DoS attacks such as report disruption attacks and selective forwarding attacks.
3) It can accommodate highly dynamic sensor networks and should not issue the process of path establishment or reparation frequently.
4) It should not rely on any fixed paths between the base station and cluster-heads to transmit messages.
5) It should prevent the uncompromised nodes from being impersonated. Therefore, when the compromised nodes are detected, the infected clusters can be easily quarantined by the base station.

IV. SYSTEM DESCRIPTION

When an event occurs within some cluster, the cluster-head collects the sensing reports from sensing nodes and aggregates them into the aggregated reports. Then it forwards the aggregated reports to the base station through forwarding nodes[4]. In our scheme, each sensing report contains one MAC that is produced by a sensing node using its authentication key, while each aggregated report contains distinct MACs, where the maximum number of compromised nodes allowed in each cluster is is point out in figure 5.

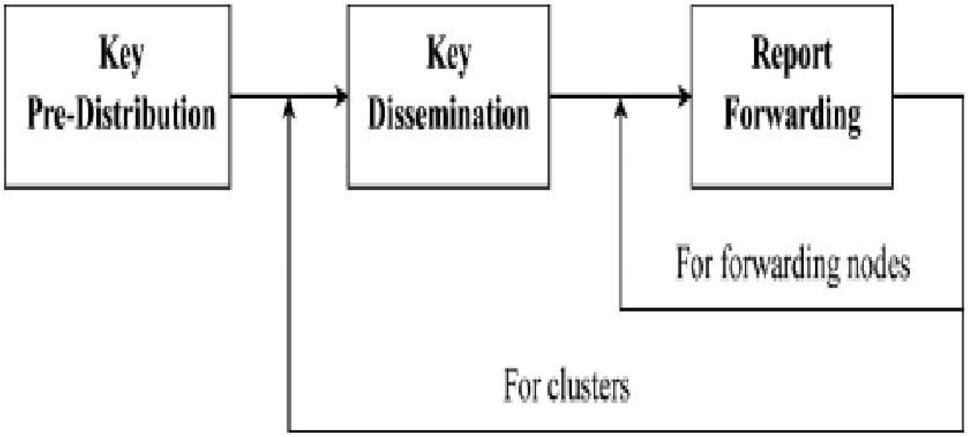

Figure 5: Relationship between phases

4.0 Key Pre-Distribution Phase

Key predistribution needs to be performed only once. Each node is preloaded with a distinct seed key. From the seed key, it can generate a sequence of auth-keys using a common hash chain[4]. The base station is aware of each node's seed key, so the adversaries cannot impersonate the uncompromised nodes. Beside the secret key, each node equipped with secret keys, are randomly chosen from another global key pool.

4.1 Key Dissemination Phase

Key dissemination is executed by clusters periodically only once. In the key dissemination phase, the cluster-head disseminates each node's first auth-key to the forwarding nodes, which will be able to filter false re-ports later. Key dissemination happens before the sensing nodes begin to send the reports. It may be executed periodically depending on how often the topology is changed[4]. Every time the latest (unused) auth-key of sensing nodes will be disseminated.

4.2 Report Forwarding Phase

Report forwarding happens at each forwarding node in every round. In the report forwarding phase, each forwarding node verifies the reports using the disclosed auth-keys and disseminated ones. If the reports are valid, the forwarding node discloses the auth-keys to its next-hop node after overhearing that node's broadcast Otherwise, it informs the next-hop node to drop the invalid reports[4]. This process is repeated by every forwarding node until the reports are dropped or delivered to the base station. Report forwarding occurs at each forwarding node in every round.

V. LIFETIME MAXIMIZATION

To improve energy- efficiency data aggregation and dissemination protocols for wireless sensor networks. Let's take an example to show how our framework can outperform other ones. Consider the two-node example shown in Figure 7. N1 and N2 are two sensor nodes and L1 and L2 are the candidate stops of the mobile sink. Suppose we ignore the receiving energy requirement and suppose the transmission energy per unit of data is equal to the square of the distance between the sender and receiver.

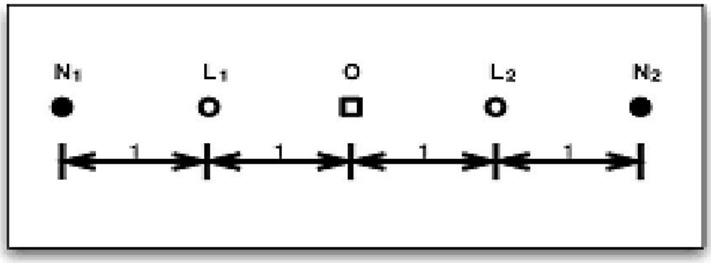

Figure 6: Mobile Sink model & Delay-Tolerant Mobile Sink Model

Both nodes N1 andN2 generate data at 1 bps and have 100 units of energy initially. If the sink is located at O in the SSM, both nodes spend 4 units of energy for sending a bit of data is shown in figure 6. It is obvious that the optimal lifetime is 24 seconds. In the MSM with sink locations fL1;L2g, due to the symmetry of the structure, the sink stays at both L1 and L2 for the same amount of time to achieve the maximum lifetime. Each node spends 1 or 9 units of energy for sending 1 bit of data depending whether the sink is at L1 or L2. The average energy consumption per bit is 4 units. Thus, the lifetime is 20 seconds. In the DT-MSM, we assume that the sink alternates between the two stops and stays for 1 second at each stop in each cycle. Hence, this is the case that D ¼ 2 seconds. When the sink stays at L1, only N1 sends 2 bits of data to the sink; when the sink moves to L2,only N2 transmits 2 bits of data (N2 keeps its data while the sink is at L1). Both nodes spend 2 units of energy every 2 seconds or 1 unit of energy per second on average. Thus, the lifetime is 100 seconds, a significant increase compared to the SSM and MSM. This is because, in the DT-MSM, the nodes do not always participate in communication for all the sink stops; they each wait until the sink's location is most favorable for energy saving, and then send data at the higher rate. Recall that we have assumed that the traffic rate is sufficiently small compared to the capacity of the wireless link, and hence, sending data at a higher rate does not alter the per-bit energy consumption.

5.0 Static Sink Model

In the static sink model (SSM), the sink is located at the origin and remains stationary during the operation of the WSN. Data originated from the sensor nodes flow into the sink in a multihop fashion. As soon as the data become available at a node, it gets transmitted toward the sink[7]. Typically, the rate at which each sensor node harvests data from the outside world is a constant. The data generated by a source are sometimes called a commodity or a subflow.

5.1 Mobile Sink Model

The sink can move to several locations to collect data. When the sink is at each location, all sensors participate in the communication, sending and relaying traffic to the sink. In the mobile sink model (MSM), we assume that the sink can move around within the sensor field and stop at certain locations to gather the data from the sensor nodes [8]. Let the set of possible locations where the sink can stop (also known as sink stops). The sink does not necessarily stop at (i.e., stays for a positive duration) all locations in the interest of maximizing the network lifetime.

5.2 Delay-Tolerant Mobile Sink Model

When the mobile sink is at a stop, a subset of the sensor nodes can participate in the communication. We use the queue-based variant of this model to evaluate the performance. We consider how to maximize the lifetime of WSN with the mobile sink in applications that can tolerate a certain amount of delay. We call the resulting WSN model as delay tolerant mobile sink model (DT-MSM)[9]. In this setting, each node can postpone the transmission of data until the sink is at the stop most favorable for extending the network lifetime. This way, the nodes can collectively achieve a longer network lifetime. In contrast, the SSM and MSM do not exploit this possibility.

VI. IMPLEMENTATION PLAN

6.0 Wireless Sensor Network Creation

This module includes the creation of wireless Network i.e. collection of nodes to be generated and placed in particular position and wireless communication will be established between the entire networks for Data Transmission.

6.1 Message Authentication

In this module sensor nodes are organized into clusters. Each legitimate report should be validated by multiple message authentication codes (MACs), which are produced by sensing nodes using their own authentication keys[6]. The authentication keys of each node are created from a hash chain. Before sending reports, nodes disseminate their keys to forwarding nodes using Hill Climbing approach. Then, they send reports in rounds. In each round, every sensing node endorses its reports using a new key and then discloses the key to forwarding nodes. Using the disseminated and disclosed keys, the forwarding nodes can validate the reports. In our scheme, each node can monitor its neighbors by overhearing their broadcast, which prevents the compromised nodes from changing the reports. Report forwarding and key disclosure are repeatedly executed by each forwarding node at every hop, until the reports are delivered to the base station.

6.2 Multipath Routing

This module includes the functionality of creating the multiple copies of the same data and transmitted to the base station via multiple paths to increase the throughput as choose application is based on delay constraint and if the data doesn't reach on time it is entirely waste of receiving the information [4].

VII. SIMULATION RESULTS

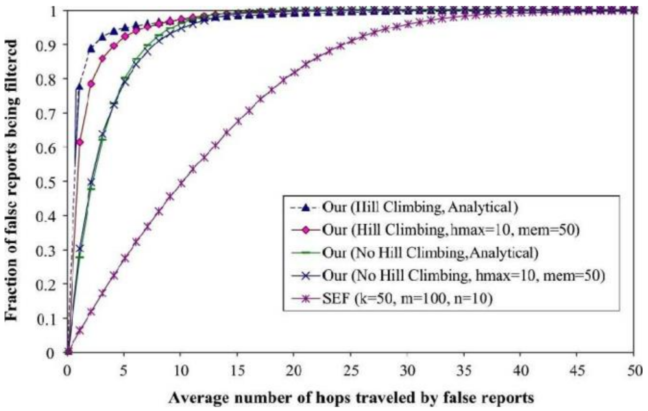

Figure 7. False reports filtered versus number of hops traveled

Our scheme drops false reports earlier even with a lower memory requirement. It can drop false reports in 6 hops with only 24 keys stored in each node. The fraction of false reports filtered increases as the number of hops that they travelled grows is illustrated in figure 8. The simulation results shown in our scheme can drop 90% of false reports within 4 hops using Hill Climbing or 10 hops without Hill Climbing.

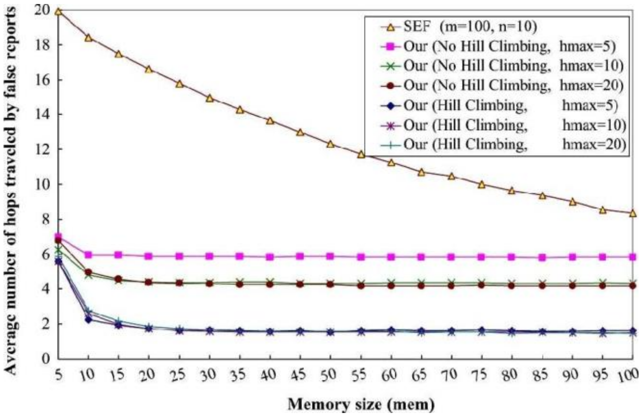

Figure 8: Filtering capacity versus memory size

Figure 9 depicts how filtering capacity varies as memory size changes, where the filtering capacity is measured as the average number of hops that a false report can travel. The smaller the number of hops, the higher the filtering capacity. Therefore our scheme outperforms even with a much lower memory requirement. Note that, in the figure 9, the lifetime is normalized with respect to the optimal lifetime of the MSM. The lifetime of the DT-MSM increases as the radius of coverage increases.

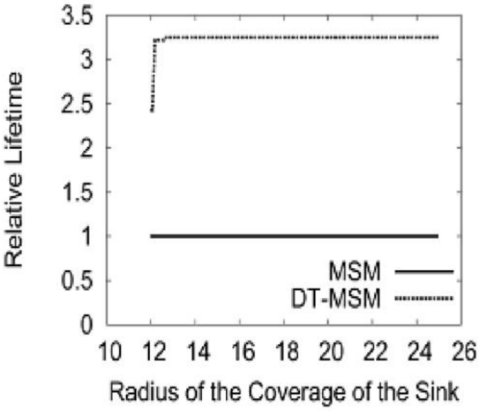

Figure 9: Lifetime under various radii of coverage

The increase is sharpest when the radius just exceeds the coverage is set large enough to always cover the entire sensor field[8].As shown in Figure 9, the lifetime of the MSM is about 100-200 percent greater than that of the SSM. However, the DT-MSM is 200-1,000 percent better than the SSM. Moreover, the curves all look linear; the performance gap can grow even larger with more sink locations. Both the MSM and the DT-MSM exhibit a sharp lifetime increase when the transmission range is small but increasing [9]. However, as the transmission range becomes large, the lifetime increase comes to a stop. This is because the energy cost increases with the transmission distance, and hence, in an optimal solution, a node does not pick faraway nodes as the next-hop neighbors even if the transmission range allows it. The observed fluctuation in the curves is due to statistical fluctuation in the samples of the random network topologies. The lifetime of the MSM and DT-MSM are normalized with respect to the optimal lifetime of the SSM.

VIII. CONCLUSION

A dynamic en-route scheme can drop false reports much earlier even with a smaller size of memory. The uncompromised nodes will not be impersonated because each node has its own auth-keys. Therefore, once the compromised nodes are detected, the infected clusters can be easily quarantined. Our Hill Climbing key dissemination approach increases filtering capacity greatly and balances the memory requirement among nodes. We also proposed a new framework for improving the network lifetime by exploiting sink mobility and delay tolerance. It is expected to be useful in applications that can tolerate a certain amount of delay in data delivery. We presented the mathematical formulations for optimizing the network lifetime under the proposed framework. We identified several properties that our models possess. The results of the paper can both be applied to practical situations and be used as benchmarks for studying energy-efficient network designs.

REFERENCES

[1] Chih-ping li and Michael J. Neely “Energy- Optimal Scheduling with Dynamic Channel Acquisition in Wireless Downlinks”, IEEE Conference on Decision and control, pp. 1140 – 1147,2007.

[2] Kui Ren, Wenjing Lou, and Yanchao Zhang,“LEDS:Providing Location-Aware End-to-End Data Security in WSN”,IEEE,pp.484 – 498,2008.

[3] Fan Ye, Haiyun Luo, Songwu Lu, Lixia Zhang, “Statistical En-route Filtering of Injected False Data in Sensor Networks”, IEEE INFOCOM, pp 2446 -2447,2004.

[4] Sencum Zhu, Sushil Jaiodia, “An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks”,IEEE Symposium on security and privacy, pp 1-13,2004.

[5] Young Sang, Ye Xia, “Maximizing the Lifetime of Wireless Sensor Networks with Mobile Sink in Delay-Tolerent Applications”,IEEE Transactions on Mobile Computing, pp 1308 – 1318,2010.

[6] Zhen Yu, Yong Guan, “A dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks”, IEEE / ACM Transaction on Networking, pp 140 – 162,2010.

[7] Z.M. Wang, S. Basagni, E. Melachrinoudis, and Petrioli,"Exploiting Sink Mobility for Maximizing Sensor Network Life-time," Proc. 38th Hawaii Int'l Conf. System Sciences, pp.484-498,2004.

[8] M. Gatzianas and L. Georgiadis, "A Distributed algorithm for Maximum Lifetime Routing in Sensor Networks with Mobile Sink," IEEE Trans. Wireless Comm., pp. 984-994, 2008.

[9] I. Papadimitriou and L. Georgiadis, "Maximum Lifetime Routing to Mobile Sink in Wireless Sensor Networks," Proc. 13th IEEE Int'l Conf. Software Telecomm. and Computer networks, pp.148-1170,2004.