En-route Filtering Scheme for Dynamic Data Reporting in Wireless Sensor Networks

M. V. N. Kuamr#1, B.P.N. Madhu Kumar#2, R.V.Satyanarayana#3

(#1 M.Tech Student, B.V.C. Engineering College, Odalarevu)
(#2 Associate Professor, Department of CSE, BVCEC, Odalarevu)
(#3 HOD of CSE Dept, BVCEC, Odalarevu)

Abstract:
In wireless sensor networks, adversaries can inject false data reports via compromised nodes and launch DoS attacks against legitimate reports. Recently, a number of filtering schemes against false reports have been proposed. 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, each node has a hash chain of authentication keys used to endorse reports; meanwhile, a legitimate report should be authenticated by a certain number of nodes. First, each node disseminates its key to forwarding nodes. Then, after sending reports, the sending nodes disclose their keys, allowing the forwarding nodes to verify their reports. 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 DoS 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.

INTRODUCTION

In these large sensor network systems, we need nodes to be able to locate themselves in various environments, and on different distance scales. This problem, which we refer to as *localization*1, is a challenging one, and yet extremely crucial for many applications of very large networks of devices.

For example, localization opens up new ways of reducing power consumed in multi-hop wireless networks. In context-aware applications, localization enables the intelligent selection of appropriate devices, and may support useful coordination among devices. The desired granularity of localization is itself application dependent. GPS [1] solves the problem of localization in outdoor environments for PC class nodes. However, for large networks of very small, cheap and lowpower devices, practical considerations such as size, form factor, cost and power constraints of the nodes preclude the use of GPS on all nodes. In this paper, we address the problem of localization for such devices, with the following design goals. *RF-based:* We focus on small nodes which have some kind of short-range radio frequency (RF) transceiver. Our primary goal is to leverage this radio for localization, thereby eliminating the cost, power and size requirements of a GPS receiver. *Receiver based:* In order to scale well to large distributed networks, the responsibility for localization must lie with the receiver node that needs to be localized and not with the reference points. *Adhoc:* In order to ease deployment, we desire a solution that does not require pre-planning or extensive infrastructure. *Responsiveness:* We need to be able to localize within a fairly low response time .*Low Energy:* Small, un-tethered nodes have modest processing capabilities, and limited energy resources. If a device uses all of its energy localizing itself, it will have none left to perform its task. Therefore, we desire to minimize computation and message costs to reduce power consumption. *Adaptive Fidelity:* In addition,we want the accuracy of our localization algorithmsto be adaptive to the granularity of available reference points.

RELATED WORK

In this paper, we propose a dynamic en-route filtering scheme 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 (MACs), 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. 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 dropped or delivered to the base station

SCHEMES OF LOCALIZATION

Many existing systems and protocols attempt to solve the problem of determining a node's location within its environment. The approaches taken to solve this localization problem differ in the assumptions that they make about their respective network and device capabilities. These include assumptions on devicehardware, signal propagation models, timing and energy requirements, network makeup (homogeneous vs. heterogeneous), the nature of the environment (indoor vs. outdoor), node or beacon density, time synchronization of devices, communication costs, error requirements, and device mobility. In this section, wediscuss prior work in localization with regard to these network characteristics, device restrictions, and application requirements.

We divide our discussion into two subsections where we presentboth range-based and range-free solutions.

1 RANGE-BASED LOCALIZATION SCHEMES

Time of Arrival (TOA) technology is commonly used as ameans of obtaining range information via signal propagation time.The most basic localization system to use TOA techniques is GPS. GPS systems require expensive and energy-consumingelectronics to precisely synchronize with a satellite's clock. With

hardware limitations and the inherent energy constraints of sensornetwork devices, GPS and other TOA technology present a costlysolution for localization in wireless sensor networks.

The Time Difference of Arrival (TDOA) technique for **ranging**(estimating the distance between two communicating nodes) hasbeen widely proposed as a necessary ingredient in localizationsolutions for wireless sensor networks. While manyinfrastructure-based systems have been proposed that use TDOA, additional work such as AHLoshasemployed such technology in infrastructure-free sensor networks.

Like TOA technology, TDOA also relies on extensive hardwarethat is expensive and energy consuming, making it less suitablefor low-power sensor network devices. In addition, TDOAtechniques using ultrasound require dense deployment as ultrasound signals usually onlypropagate 20-30 feet.To augment and complement TDOA and TOA technologies, anAngle of Arrival (AOA) technique has been proposed that allowsnodes to estimate and map relative angles between neighbors.Similar to TOA and TDOA, AOA estimates require additionalhardware too expensive to be used in large scale sensor networks.Received Signal Strength Indicator (RSSI) technology such as RADAR and SpotOn has been proposed for hardwareconstrainedsystems. In RSSI techniques, either theoretical orempirical models are used to translate signal strength into distance estimates. For RF systems, problems such as multi-pathfading, background interference, and irregular signal propagationcharacteristic make range estimates inaccurate. Work to mitigate sucherrors such as robust range estimation, two-phaserefinement positioning, and parameter calibrationhave been proposed to take advantage of averaging,smoothing, and alternate hybrid techniques to reduce error towithin some acceptable limit. While solutions based on RSSIhave demonstrated efficacy insimulation and in a controlledlaboratory environment, the premise that distance can be determined based on signal strength, propagation patterns, andfading models remains questionable, creating a demand foralternate localization solutions that work independent of thisassumption.

2 RANGE-FREE LOCALIZATION SCHEMES

In sensor networks and other distributed systems, errors canoften be masked through fault tolerance, redundancy, aggregation,or by other means. Depending on the behavior and requirementsof protocols using location information, varying granularities oferror may be appropriate from system to system. Acknowledgingthat the cost of hardware required by range-based solutions maybe inappropriate in relation to the required location precision,researchers have sought alternate range-free solutions to thelocalization problem in sensor networks.In ,a heterogeneous network containing powerful nodeswith established location information is considered. In this work,anchors beacon their position to neighbors that keep an account ofall received beacons. Using this proximity information, a simple centroid model is applied to estimate the listening nodes' location.We refer to this protocol as the *Centroid algorithm.*An alternate solution, *DV-HOP* assumes a heterogeneousnetwork consisting of sensing nodes and anchors. Instead ofsingle hop broadcasts, anchors flood their location throughout thenetwork maintaining a running hop-count at each node along theway. Nodes calculate their position based on the received anchorlocations, the hop-count from the corresponding anchor, and theaverage-distance per hop; a value obtained through anchorcommunication. Like DV-Hop, an *Amorphous Positioning*algorithm proposed in uses offline hop-distance estimations,improving location estimates through neighbor informationexchange.These range-free techniques are described in more depth insection 4, and are used in our analysis for comparison with ourwork.

3. APIT LOCALIZATION SCHEME

In this section, we describe our novel area-based range-freelocalization scheme, which we call APIT. APIT requires aheterogeneous network of sensing devices where a smallpercentage of these devices (percentages vary depending onnetwork and node density) are equipped with high-poweredtransmitters and location information obtained via GPS or someother mechanism. We refer to these location-equipped devices as**anchors**. Using beacons from these anchors, APIT employs a novel *area-based* approach to perform location estimation byisolating the environment into triangular regions betweenbeaconing nodes (Figure 1). A node's presence inside or outside\ of these triangular regions allows a node to narrow down the areain which it can potentially reside. By utilizing combinations ofanchor positions, the diameter of the estimated area in which anode resides can be reduced, to provide a good location estimate.

GOALS

We require that each report be attached with MACs generated by different sensing nodes using their own authentication keys. A false report is defined as one that contains less thanvalid MACs. Here, selecting different values of gives us a tradeoff between security and overhead. To tolerate more compromised nodes, we can increase the value of, which will incur higher communication overhead because the reports be- come longer.

As we discussed, adversaries can launch false report injection attacks and DoS attacks. Our objective is to design a scheme to detect these attacks or mitigate their impact. Compared to existing ones, our scheme is expected to achieve the following 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 asreport disruption attacks and selective forwarding attacks.
3) It can accommodate highly dynamic sensor networks and should not issue the process of path establishment or repa- ration 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 im-personated. Therefore, when the compromised nodes are detected, the infected clusters can be easily quarantined by the base station.

OVERVIEW OF THE WORK

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. In our scheme, each sensing report contains one MAC that is produced by a sensing node using its authentication key (called auth-key for short), while each aggregated report contains dis- tinct MACs, where is the maximum number of compromised nodes allowed in each cluster. In our scheme, each node possesses a sequence of auth-keys thatform a hash chain. Before sending the reports, the cluster-head disseminates the first auth-keys of all nodes to the forwarding nodes that are located on multiple paths from the cluster-head to the base station. The reports are organized into rounds, each containing a fixed number of reports. In every round, each sensing node chooses a new auth-key to authenticate its reports. To facilitate verification of the forwarding nodes, the sensing nodes disclose their auth-keys at the end of each round. Meanwhile, to prevent the forwarding nodes from abusing the disclosed keys, a forwarding node can receive the disclosed auth-keys, only after its upstream node overhears that

it has already broadcast the reports. Receiving the disclosedkeys, each forwarding node verifies the reports, and informs its next-hop node to forward or drop the reports based on the verification result. If the reports are valid, it discloses the keys to its next-hop node after overhearing. The processes of verification,overhearing,andkeydisclosureare repeated by the forwarding nodes at every hop until the reports are dropped or delivered to the base static Specifically, our scheme can be divided into three phases:key predistribution phase, key dissemination phase, and report forwarding phase. In the key predistribution phase, each node is preloaded with a distinct seed key from which it can generate a hash chain of its auth-keys. 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. 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. This process is repeated by every forwarding node until the reports are dropped or delivered tothe base station.

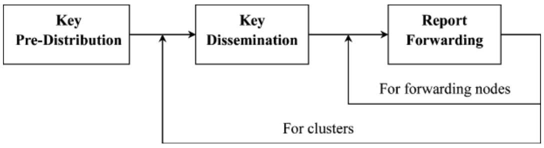

Fig1 The relationship between three phases of our scheme. Key pre-distribution is preformed only once. Key dissemination is executed by clusters periodically. Report forwarding happens at each forwarding node in every round.

Fig 1 demonstrates the relationship between the three phases of our scheme. Key predistribution is performed before the nodes are deployed, e.g., it can be done offline. Key dissemination happens before the sensing nodes begin to send the reports.Itmaybe executed periodically depending on how often thetopology is changed. Every time the latest (unused) auth-key of sensing nodes will be disseminated. Report forwarding occurs at each forwarding node in every round

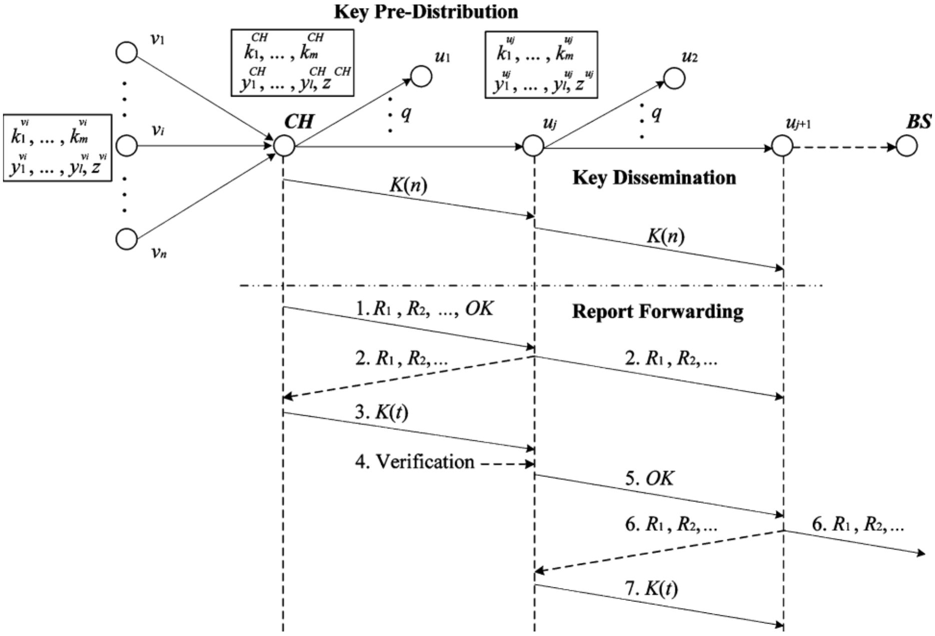

Fig.2 The detailed procedure of three phases

.

In the *key predistribution phase*, each node is preloaded with l+1 secret keys .y1….yn and z, and can generate a hash chain of auth-keys k1…kn from the seed key km. In the *key dissemination phase*, the cluster-head disseminates the auth-keys of all nodes by message k(n) to q downstream neighbor nodes. Every downstream node decrypts some auth-keys from k(n), and further forwards K(n) to q more downstream neighbor nodes, which then repeat the same operation. In the *report forwarding phase*, each forwarding node en-route performs the following steps: 1) It receives the reports from its upstream node. 2) If it receives confirmation message OK then forwards

the reports to its next-hop node. Otherwise, it discards the reports. 3) It receives the disclosed auth-keys within message k(t)and verifies the reports by using the disclosed keys. 4) It informs its next-hop node the verification result.

SIMULATION RESULTS

In summary, simulation results show that our scheme has the following advantages when compared with others:

1)Our scheme drops false reports earlier even with a lower memory requirement. In some scenario, it can drop false reports in 6 hops with only 25 keys stored in each node, but another scheme needs 12 hops even with 50 keys stored.

2) Our scheme can better deal with the dynamic topology ofsensor networks. It achieves a higher filtering capacity and filters out more false reports than others in dynamic net- work.

3) Hill Climbing increases thefiltering capacity of our scheme greatly and balances the memory requirement among sensor nodes.

CONCLUSION

In this paper, we propose a dynamic en-route quarantine scheme for filtering false data injection attacks and DoS attacks in wireless sensor networks. In our scheme, each node uses its own auth-keys to authenticate their reports and a legitimate report should be endorsed bynodes. The auth-keys of each node form a hash chain and are updated in each round. The cluster-head disseminates the first auth-key of every node to forwarding nodes and then sends the reports followed by disclosed auth-keys. The forwarding nodes verify the authen- ticity of the disclosed keys by hashing the disseminated keys and then check the integrity and validity of the reports using the disclosed keys. According to the verification results, they inform the next-hop nodes to either drop or keep on forwarding the reports. This process is repeated by each forwarding node at every hop.

FUTURE WORK

In future, we will study how to take advantage in our scheme of various energy-efficient data aggregation and dissemination protocols for wireless sensor networks.

REFERENCES

[1] D. Braginsky and D. Estrin, “Rumor routing algorithm for sensor networks,”in *Proc. WSNA*, 2002, pp. 22–31.

[2] N. Bulusu, J. Heidemann, and D. Estrin, “GPS-less low cost outdoor localization for very small devices,” *IEEE Personal Commun. Mag.*,

[3] S. Capkun and J. Hubaux, “Secure positioning of wireless devices withapplication to sensor networks,” in *Proc. IEEE INFOCOM*, 2005, vol.3, pp. 1917–1928.

[4] L. Eschenauer and V. Gligor, “A key-management scheme for distributed sensor networks,” in *Proc. ACM CCS*, 2002, pp. 41–47.
[5] T. He, C. Huang, B. Blum, J. Stankovic, and T. Abdelzaher, “Rangefree localization schemes in large scale sensor network,” in *Proc. ACM MobiCom*, 2003, pp. 81–95.
[6] C. karlof and D.Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” in *Proc. 1st IEEE Int.Workshop Sensor Netw. Protocols Appl.*, 2003, pp. 113–127