Secret Sharing and Node Mobility in UWSN

Parashakthi S

M.TECH in Computer Networks, Shree Devi Institute of Technology, Kenjar, Mangalore, Karnataka, India

Abstract: In recent years, wireless sensor networks (WSNs) have been a very popular research topic which helps in networking, hardware, security and application-related problems. In this paper we focus on Mobile Unattended Wireless Sensor Networks (MUWSNs), nodes sense the environment and store the acquired data until the arrival of a trusted data sink. In this paper, we address the fundamental issue of quantifying to which extent secret sharing schemes, combined with nodes mobility, can help in assuring data availability and confidentiality. Secret sharing and node mobility can help in assuring data security using local communications only, and understanding how to set system parameters to achieve the desired trade-off between confidentiality and availability. We provide accurate analytical results binding the fraction of the network accessed by the sink and the adversary to the amount of information they can successfully recover. Extensive simulations support our findings.

Keywords: Mobile Unattended Wireless Sensor Networks (MUWSNs); Unattended Wireless Sensor Networks (UWSN); privacy, metrics, mobility models.

I. INTRODUCTION

The main concerns for MUWSNs are data availability and confidentiality, i.e., to avoid that stored data are lost, due to nodes failure or capture, or exposed to unauthorized entities. The issues are the distributed nature of the network, the Remarkable constraints in energy supply, storage capacity and computational power of the nodes, and the possible presence of active adversaries. In particular, the amount of data handled by any sensor's transceiver should be minimized, because transmission and reception of a message are much more expensive operations than data elaboration.

In proposed system we define a very energy-efficient scheme that relies on local secret sharing and leverages the mobility of the nodes to provide information diffusion. Assuming data is spatially diffused, we provide a thorough analysis of the shares recovery process, deriving bounds on the amount of data that can be reconstructed after all the shares stored by a given fraction of the nodes has been collected. This means that we can accurately foresee how much information can be recovered by both the sink and the adversary as a function of their capabilities and of the parameters of the scheme. To simulate the behavior of the network, we chose three mobility models from the literature. The experiments validate our analysis and provide remarkable insights on the proposed scheme. Further, we provide precise indications about how the parameters of sharing schemes should be chosen according to the mobility degree of the network, to the capabilities of both the sink and the adversary, and to the desired levels of availability and confidentiality.

II. SCENARIOS

The Network: N sensor nodes, denoted $s1, \ldots, sN$, are randomly deployed in an $L \times L$ square area A. Each node si moves randomly in A, storing the data sensed (Di) in a radius r around it — $Di \in$ □q, for a suitable q. At regular intervals, a trusted mobile sink explores a portion of A, recovering all data stored by the nodes in its communication range, which right after are securely deleted. During the sink absence, there is no centralized control and the network works in a totally distributed way.

The Adversary: We assume that the adversary can both eavesdrop the communications between any two nodes of the network and corrupt nodes to access all the data and key material they store. However, assuming the use of symmetric key encryption, the adversary can only read data received and stored by the corrupted nodes, for which it has access to the key. Observe that, if the amount of sensed, plaintext, data available to the adversary was the same available to the sink, no scheme could provide both availability and confidentiality.

III. SYSTEM ARCHITECTURE

Mobile Sink (Sink): In this module is a mobile sink sends data request messages to the sensor nodes via a stationary access node. These data request messages from the mobile sink will initiate the stationary access node to trigger sensor nodes, which transmit their data to the requested mobile sink

Public Key Security Scheme: In this module is a Public Key Based Security Model, we present the Key Based Security the process of the secure data sharing between the nodes.

Sensor nodes: In this module based on the polynomial pool-based key pre-distribution scheme substantially improved network resilience to mobile sink replication attacks compared to the single polynomial pool-based key pre-distribution approach. Using two separate key pools and having few stationary access nodes carrying polynomials from the mobile pool in the network may hinder an attacker from gathering sensor data, by deploying a replicated mobile sink.

Access node replication: In this module we have strengthened the authentication mechanism between the stationary access nodes and sensor nodes using one-way hash chains algorithm in conjunction with the static polynomial pool-based scheme. They developed a general framework for pair-wise key establishment using the polynomial-based key pre-distribution protocol and the probabilistic key distribution in 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 the network sensor nodes, making it possible for the attacker to take control of the entire network by deploying a replicated mobile sink, preloaded with some compromised keys to authenticate and then initiate data communication with any sensor node.

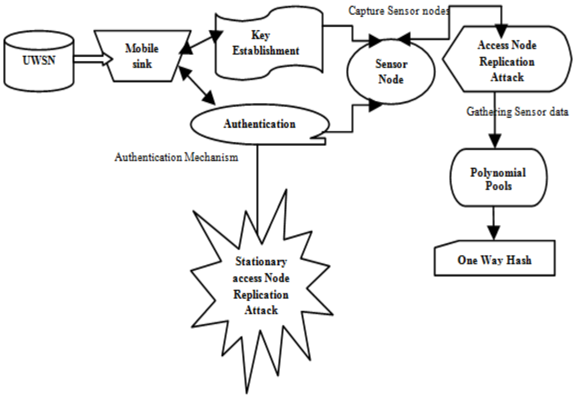


Figure1: System architecture

IV. SCHEME DESCRIPTION

Let *Di,t* ∈ □*q* be the data sensed by *si* at a given time *t*. Since our analysis only focus on the time window between *t* and the arrival of the sink or the adversary, we can ease the notation and refer *Di,t* as *Di*.

Shares Generation: *si* implements a (*k*, *n*) sharing scheme over □*q*, obtaining from *Di* the *n* shares *D*1 *i* , . . . , *Dn i* .

Local Distribution: *si* randomly selects *n*−1 neighboring nodes *si*1, . . . , *sin*−1 , sends one of the shares to each of them, keeping the last share for itself, and securely deletes *Di*.

Information Diffusion: Each secret *Di* is now shared among the nodes *si*, *si*1, . . . , *sin*−1 , so that all nodes now store shares of different secrets. Thanks to sensors' random movement, the information gets then spatially spread in *A*.

Data Collection: The sink starts exploring *A* at time *t*+*τS*. As a node enters its communication range, all the shares it stores are offloaded to the sink and promptly deleted from the memory of the sensor. The sink stops and leaves the network as soon as it meets a predefined number of nodes *mS*.

LEVEL-1

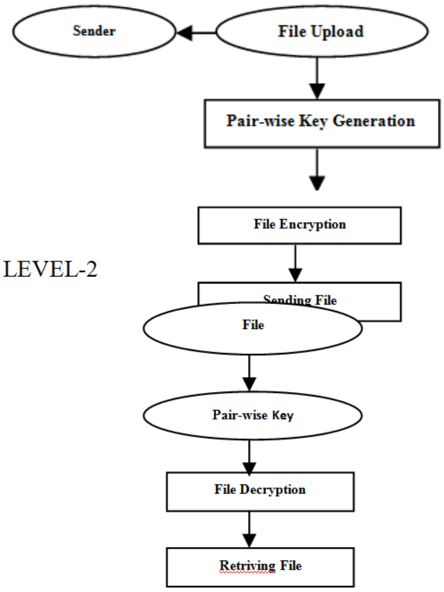


Figure2 : Data flow diagram

Remark 1. The adversary starts exploring A at time t + Ta and corrupts all the nodes it meets, collecting the shares they store. To avoid the sink, it must leave the network quickly, so it can corrupt a number of nodes mA remarkably smaller than mS. Previously captured nodes being recoverable through centralized or distributed healing schemes, we can assume that only data stored by the mA newly corrupted sensors are accessible to the adversary.

Remark 2. The implicit requirement of (n − 1)-connectivity can be relaxed leveraging the mobility of the nodes, by letting them distribute the shares within a sharing interval τ > 0. Indeed, the configuration of the network can be modelled as a random geometric graph and we can set n so as to ensure that every node has always at least n−1 neighbors with probability at least 1 − _. In fact, we can compute

n = 1+max{m : Pr[degmin < m− 1] < _} (1)

based on the density and communication range of the nodes ([1]), where degmin is the minimum degree of the network. If deg(si) < n− 1, si can ask some neighbors to route the exceeding shares to their own neighbors. Table I summarizes the routing required during the shares distribution in our 72000 simulations.

n was set according to Eq. (1), where € = 10−4, and we assumed the network composed of N = 500 nodes. As expected, routing was de facto non-necessary or negligible.

V. MAIN RESULTS

The core of our analysis concerns the distribution of the number of secrets that can be recovered from the shares stored by a given fraction of the network. Our main results, stated in Theorem 1**,** consist in two bounds for the tails of this distribution.

De facto, they represent a lower and an upper bound on the performances of the sink and the adversary, respectively, thus providing a quantitative analysis of the reliability and confidentiality ensured by our scheme.

From here on, Poiλ(E) and Binl,p(E) denote the probability of event E for a Poisson of mean λ and a Binomial of parameters l and p, respectively.

Theorem 1. Assume that all data sensed at time t were locally shared according to the scheme of Sect. IV. Let Sink≤ h denote the event "the sink recovers at most h secrets", and Adv≥ h the event "the adversary recovers at least h secrets". Let μ(m) = mn/N and p(m) = Poiμ(m) ([k,+∞)).

1. If at time t + τS the position of each node is uniformly distributed in A and independent from its position at time t, then
Pr[Sink≤ h] ≤ 2BinN,p(mS) ([0, h]) . (2)
As a consequence, for all h < Np(mS),

Pr[Sink≤ h] ≤ 2(Np(mS)H)he −(Np(mS)−h) . (3)

2. If at time t + τA the position of each node is uniformly distributed in A and independent from its position at time t, then
Pr[Adv≥ h] ≤ 2BinN,p(mA) ([h,N]) . (4)
As a consequence, for all h > Np(mA),

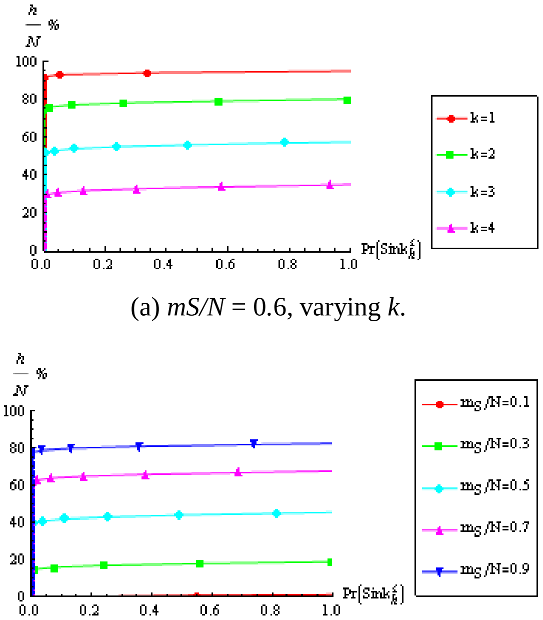
Pr[Adv≥ h] ≤ 2 (Np(mA) h)h eh−Np(mA) . (5)

Bounds (3) and (5) are weaker than (2) and (4), but more explicit. Figs. 1 and 2 show how (2) and (4) depend on *k*, *mS* and *mA*, with *N* = 500, *r* = 0.15 and *n* = 5 fixed.

Observe that the probability distribution of the number of recovered secrets is very *concentrated* around its expected (and most probable) value.

For example, if a (3, 5) secret sharing scheme is implemented, the sink meeting the 60% of the network recovers with very high probability approximately the 55% of the sensed data, while an adversary corrupting the 10% of the network recovers with very high probability approximately the 2.5% of the sensed data (figs. 1a and 2a).

Note how this means that the (3, 5) scheme actually meets the target, since the sink only loses approximately the 10% of its efficiency, compared to the 75% efficiency loss of the adversary



(a) *mS/N* = 0.6, varying *k*.

(b) *k* = 3, varying *mS/N*.

Figure 3: Percentage of data recovered by the sink, according to Eq. (2).

VI. CONCLUSION

In this paper we focused on information availability and confidentiality via secret sharing in UWSN. We bounded the amount of information retrievable by the sink and by the adversary, as a function of the parameters *k* and *n* of the secret sharing scheme and of the accessed fraction of the network. This result allows to properly choose the ratio between *k* and *n* to obtain the desired trade-off between data reliability and privacy. We performed extensive simulations, whose results support our above findings. Further, we empirically showed and discussed the impact of mobility in an UWSN, with respect to data availability and confidentiality.

REFERENCES

[1]. C. Bettstetter, "On the Minimum Node Degree and Connectivity of a Wireless Multihop Network", Proc. of the 3rd ACM Int. Symp. On Mobile Ad Hoc Networking and Computing (MOBIHOC '02), EPF Lausanne, Switzerland, June 9-11, 2002, pp. 80 91.

[2]. Y. Ren, V. Oleshchuk and F.Y. Li, "A Distributed Data Storage and Retrieval Scheme in Unattended WSNs Using Homomorphic Encryption and Secret Sharing", Wireless Days, 2009 2nd IFIP, Paris, Dec. 2009.

[3]. Q. Wang, K. Ren, W. Lou and Y. Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance", Proc. of the 28th Annual IEEE Int. Conf. on Computer Communications (INFOCOM '09), IEEE, April 2009.