International Journal of Smart Business and Technology
Vol. 1, No. 1, (2013), pp.1-16
http://dx.doi.org/10.21742/ijsbt.2013.1.1.01

A Privacy Preserving Scheme in Wireless Sensor Networks

Xiao Shijie[1], Shekhar Verma[2], Ashmita Debnath[3] and Geetam S Tomar[4]

[1]*Department of Information Science and Electrical Engineering, ShanDong JiaoTong University, Jinan, Shandong, China*
[2,3]*Dept of CSE, Indian Institute of Information Technology, Allahabad India*
[4*]*Dept of Electrical and Computer Engg, University of West Indies, St. Augustine, Trinidad & Tobago*
[1]*worldxiao509@126.com,* [2]*sv.iiitm@gmail.com,* [4]*gstomar@ieee.org*

Abstract

The privacy of sensitive events observed by a sensor network needs to be protected. An adversary can track the trajectory of a moving object or determine the location of the occurrence of a critical event to breach its privacy. In this paper, we propose a ring signature for obfuscating spatial information. First, the extended region of location of an event of interest as estimated from a sensor communication is presented. Then, the increase in this region of spatial uncertainty due to the effect of a ring signature is determined. We observe that ring signature can effectively enhance the region of location uncertainty of a sensed event. This can help in sustaining the privacy of the event of interest against a local or a global adversary. Finally, we evaluate the efficacy of our privacy enhancing strategy by finding its effect on the delay and throughput of the sensor network.

Keywords: *Privacy, Wireless sensor network, Ring signature*

1. Introduction

A typical task of any wireless sensor network is to send time-critical data to a centralized authority namely the base station. The critical nature of data acquired by a sensor node is its rigid time criticality and spatial significance. Data sensed by a sensor node needs to be sent to the base station through a secure communication channel [1]. Impairment to the communication channel can lead to false alarms. Such an alarm prompts the sink to take some wrong action. Events can be generated randomly anywhere in the network or nodes can sample their environment at a certain time interval; which means networks can be either event-driven or time-driven. In event-driven networks, whenever a message is propagated through the network to the sink, message authentication both in terms of data origin and content is imperative [2]. Sensor nodes observe events and send their recordings over the network. Using this, adversaries can construct the topology of the network, node deployment details, and track the spatial-temporal evolution of events. Even if the messages are encrypted, adversaries can learn about the network by recreating the context from the temporal and spatial flow of messages [3]. This compromises the security and privacy of the network and most importantly the sensed object. This compromise may be used maliciously. For example, an animal moving in a forest may be tracked by poachers by breaching both the spatial and temporal privacy of the sensed animal by monitoring the messages in the network [4]. To protect the privacy of the sensed object, the

Article history:
Received (August 15, 2013), Review Result (October 16, 2013), Accepted (November 10, 2013)

Print ISSN: 2288-8969, eISSN: 2207-516X IJSBT

spatial information from the messages along with temporal information that yields the time of occurrence of events must be cloaked [5]. Several mechanisms have been proposed to protect the temporal context of the messages [6] [7]. These include the introduction of random time delays etc [6]. In this work, we concentrate on the mechanism for the protection of the network's spatial context so that the location of an event's occurrence cannot be learned from the information available from messages or message flows. For example, in wildlife monitoring, a target animal can be tracked by an adversary who can associate the time and place of origin of messages with the movement behavior of the animal. Thus, breaking the association of message flows from the location is imperative for sustaining the privacy of static or mobile sensed objects.

There are two privacy concerns for sensor networks, data-oriented, and context-oriented privacy. Data-oriented privacy [8] deals with securing the integrity of data gathered and transmitted to the destination. Context-oriented privacy [9] prevents adversaries from gaining access to data context information, such as the time and location where the data originated. A passive adversary eavesdrop communication between nodes to determine the location of nodes or track the evolution of events. This kind of unlawful behavior can be mitigated by using cryptographic schemes. Active malicious nodes can inject polluted information into the network through these nodes. The main focus of context-oriented privacy is to ensure the privacy of context-related information such as location and time. Location can refer to node location or data origin location. If an adversary can detect the location of the sink or the area where the event has occurred then it can breach their privacy. It may also track or compromise a sensitive critical target. Ensuring temporal privacy is also critical as the time of occurrence can lead to the origin of data. If an attacker gets information of the time of occurrence, it can easily induce important information from the network. For example, in mobile target tracking, an adversary would try to get the time when the target passes through a particular zone to deduce its movement pattern. Securing context-sensitive data can be done in two ways: securing the location of sensor nodes and data sources and hiding the time of occurrence of event generation. To sustain the privacy of the event or the nodes, the data (sensed data or data in messages) and the source of data (event or sensor node) must be protected by blurring the information and decorrelating the data from the location and time of occurrence. In this work, we employ ring signature to preserve the spatial privacy of the sensed object. This is achieved by hiding the identity of the reporting sensor node in the crowd of other nodes to obfuscate the location of the data origin.

The rest of the paper is organized as follows. Section II describes the work related to the present study. In section III, the system model along with the problem definition is given followed by the proposed scheme in section IV. Section V contains the results with the conclusion in section VI.

2. Related work

The problem of privacy preservation is addressed by perturbing the parameters being monitored. The underlying probability distributions are changed so that no definite patterns can be constructed from the perturbed data and the relations between different entities are uncorrelated [10][11][12]. Privacy is also achieved by increasing entropy [13] by enhancing the crowd size [13] or the diversity [14]. This can be achieved by employing cryptographic or non-cryptographic mechanisms [13] [14]. Some noncryptographic mechanisms have been studied in the literature [14]. The random walk has been used in Phantom routing [15] and randomized routing [16] has been used along with flooding to

hide the location of the source. Fake message injection [17] and path perturbation algorithms are also used to randomize traffic patterns and reduce the probability of tracking mobile targets. The data are aggregated or their coarseness is increased. Techniques to increase coarseness associated with location details have also been proposed. Cryptographic techniques for privacy complement the non-cryptographic techniques such as routing, virtual ring creation, etc. The choice of cryptographic techniques is important as they consume the resources of the network. This may adversely affect the latency, throughput, and network lifetime. There are many approaches to provide privacy of nodes and data while ensuring efficient resource consumption. In authors have proposed a new time-efficient source privacy scheme TESP2 against traffic analysis attack of a global eavesdropper able to monitor and analyze the traffic in the whole network. Energy-efficient data privacy protection scheme ensures privacy and security of the sensed data while maximizing the network lifetime. The energy balancing scheme is based on the distance of the nodes from the sink thus increasing the lifetime of the network. The privacy of the sensor readings is achieved through an anonymity scheme that is based on hiding the source node identity along the transmission path and only the base station can verify the sender. Identity-based ring encryption (IBRSC) has been proposed. The framework of the IBRSC scheme consists of four phases.*Setup(k*), *Keygen(IDi), Signcrypt(m, Sr, R, IDA)* and *Unsigncrypt(σ, SA)*. In the setup phase, with the security parameter *k*, the private key generator (PKG) of the system generates the public parameters π and the master secretes the key of the system. The secret key s $\in Z_q^*$ and the public parameters of the system are defined as π = { *q, G1, G2, ê, P, Ppub, H0, H1, H2, H3*},*l* is the plain text of the message. In the ID generation phase, given the identity *Idi*, The public key generator computes the corresponding private key *Si* using the public parameters and the secret key *s* and finally shares it to an *Idi* through a secure channel. The Signcrypt phase is related to the generation of the ring and creates the ciphertext. In this phase, a sender having identity *Idr* sends and runs the algorithm to send a message to the receiver having Identity ID_A. The algorithm forms the group of ring members $\{ID_1, ID_2, ID_3, ...ID_n\}$ which consists of the actual signer *Idr*. This outputs the ciphertext σ, which is to be communicated. The encrypted message σ is sent to the receiver ID_A.

3. System model and problem definition

In a WSN, sensor nodes are deployed in a region close to the event to be observed and interact with their physical environment and other nodes. These regions of deployment are usually accessible and sensed objects may be sensitive. The observation of an event of interest and communication of this information makes the sensed object susceptible to physical attacks by compromising its privacy. Thus, spatial and temporal privacy must be central to the design of such systems. The revelation of the time of occurrence breaches temporal privacy while disclosure of location compromises spatial privacy. For delay-tolerant applications, temporal privacy can be preserved by buffering the messages for random periods on intermediate nodes.

An event of interest is delay intolerant in the sense that observations of the sensor nodes warrant action immediately in a time-limited period and additional delays cannot be introduced in communication paths. The message payload containing the observations and other spatial-temporal information is encrypted to guarantee confidentiality. The header is in clear text and contains the identity of the origin, routing information, etc.

The adversary is protocol and deployment aware. It has information on the topology and current communication in the network. An adversary can eavesdrop on communication and read the clear text header information and get the identity of the source. However, it is non-intrusive and does not interfere in the functioning of the network. It does not inject or modify messages, compromise sensor nodes, or change routing paths. These passive local adversaries may collude themselves over covert channels to obtain global information of the topology and communication and act globally as global adversaries. Preservation of spatial-temporal privacy for delay intolerant applications against local and global adversaries raises additional challenges.

Problem Definition: There is a densely deployed wireless sensor network in which more than one sensor node observes an event of interest. In this delay intolerant network, the nodes transmit their observations towards the sink with minimal delay. An adversary can eavesdrop and examine messages from different sensor nodes that report the event to determine the location of the event. The problem is to hide the location information of the reporting nodes such that even an en-route adversary that gets messages from multiple sensor nodes is not able to determine the location of the event from the location information of the nodes with sufficient accuracy.

4. Spatial privacy

4.1. System model

We consider the sensors S = {S1, S2, S3,.....Sx} are deployed where x is the population of the deployed sensors. Nodes are assumed to be deployed in uniform random distribution. Before deployment, each sensor is assumed to be loaded with a public/private keypair (P_i, S_i), for $i= 1,2,3,4,.... x$. Among the public key cryptosystems available, we assume to us ID-based public-key cryptography.

There exist both local adversaries and global adversaries. The local adversary has limited access to the network information and can monitor traffic from its one-hop neighbors. Unlike the local adversary, the global adversary can have information related to the whole network. It can monitor the whole network and access local adversaries as well. Local adversaries can also collude and give information to global adversaries.

4.2. System evaluation

In a wireless sensor network, nodes are randomly scattered over a specific area so that every point in the region is within the sensing range of at least one node. The locations of the nodes in this random network follow a spatial stochastic distribution. This arrangement is usually taken to be a homogenous Poisson point process of density λ and the number of nodes in any set A of Lebesgue measure $|X|$ is Poisson with mean $\lambda|X|$. However, when the number of nodes deployed in a region is fixed, the Poisson point process is not a good representation of the node distribution. The model may give more nodes than actually present especially with the number of nodes being small. When a fixed and finite (say N) number of nodes are independent and identically distributed in a region, the point process is a binomial point process. When N points in a compact set Ware are distributed independently and uniformly, then the process is a binomial point process. For any subset $X \subset W$, the number of points in X is binomial $(n, p)$with parameters $n = N$ and $p = |X \cap W|/|W|$.

The occurrence of an event of interest or sensed object which lies in the sensing region of sensor nodes triggers communication from these nodes. A message emanating from a source

node reports an event is heard by adversaries within the node's communication range. An individual adversary or adversaries can collude to obtain a rough estimate of the location of the sensed object. This estimated zone Z is the anonymity zone. The level of anonymity of a sensed object or event is the inability of the adversary to pinpoint its location in the anonymity zone Z. The degree of anonymity of the sensed event is a function of the location uncertainty of the sensor node reporting the event. This is, in turn, proportional to the area of the anonymity zone $A(Z)$. If p_i is the probability that the event occurs at a given point in Z, then $\sum p_i = 1$.

The entropy of the distribution of the anonymity set is

$$H(p) = -\sum_{i=1}^{A(Z)} p_i \log_2 p_i$$

The anonymity of a given event is maximized when all points are equally likely to be the potential point of occurrence of the event of interest. Under this uniform distribution, the probability p_i that a point Z under observation is the target becomes

$$p_i \propto \frac{1}{A(Z)} \quad \forall A(Z) \subset W$$

Following the definition of the level of anonymity given, we have,

$$A_l = 1 - 1 / |A(Z)|$$

with entropy $H(p) = -\log_2 A(Z)$. The entropy of the anonymity set is the measure of the privacy of a sensed object or event.

If the events form a binomial point process, then the events of interest would be binomially distributed in the area $A(Z)$. The probability p_z^k that k events of interest of the point process occur in the region Z is defined as the probability of there being k points in an arbitrary set Z. If N nodes are distributed over a set W, then

$$p_z^k = \binom{N}{k} \frac{|A(Z) \cap W|^k}{|W|} \left(1 - \frac{|A(Z) \cap W|^{N-k}}{|W|}\right)$$

In a wireless sensor network, an event of interest may be observed by more than one sensor node. An adversary in the network may be aware of the node deployment or may not be aware of the node locations. A deployment unaware adversary gauges the location of the nodes from the signals broadcast by the nodes. A deployment-aware adversary knows the locations of the sensor nodes.

Case I: The adversary is deployment aware

A. The Source is known

A sensor node observes an event and transmits a message to report the event to the sink. The broadcast is received by an adversary who is in the communication range R_c of the sensor node. The adversary receives the message and reads the contents of the clear

text header to find the source of the communication. The event of interest must lie in the sensing range R_s of this source sensor node. To ensure communication connectivity $R_c \geq 2R_s$, hence, the location of the event must be within a circular region centered at the sensor node with a radius $of\ R_s$ as shown in Figure 1. This is the anonymity zone Z for the event. The event of interest would be located in Z. The area of Z would be πR_S^2.

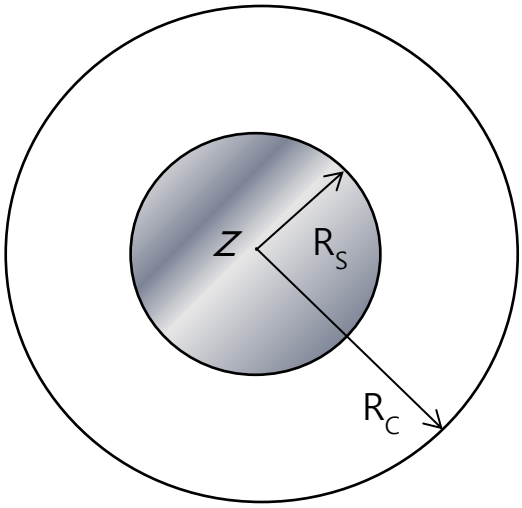

Figure 1. Anonymity zone (location of source node - known)

B. The source is not known

If the adversary is not able to determine the location of the source of the message, then the anonymity zone Z becomes the union of the sensed region of all possible source node locations as estimated by the adversary. It is clear that that the size of Z is larger as compared to the first case. Thus, the privacy of an event of interest can be increased by hiding the identity of the sensor node reporting the event.

C. Intersection Attack

The source does not know the source of a message. However, multiple sensors report events that occur in their vicinity by transmitting packets to the sink over the network. These packets are routed towards the sink by different nodes in the network. As the packets reach the destination, the routing paths may merge. An adversary sitting at a particular location in the network may receive messages from multiple sources. The possibility becomes higher if the adversary is near the sink. It is also possible that different adversaries communicate with one another over some private channels. The adversaries are aware of the location of nodes and the occurrence of an event of interest is reported without any delay. This may allow an intersection attack by an adversary receiving messages on a merged path within a small-time interval or by adversaries colluding to exchange such information. The intersection attack reduces the region of uncertainty and allows an adversary to confine the search for the event of interest to a very narrow region.

Case II: The adversary is unaware of the node deployment

A sensor node observes an event and transmits a message to report the event to the sink. The broadcast is received by an adversary who is in the communication range R_c of the sensor node. The adversary estimates the rough location of the sensor node from the received signal strength. Due to the noise and variation in signal attenuation in the wireless channel, the estimated node location may be quite inaccurate. Since a node can sense an event in a circular region of radius R_s around it, the anonymity zone Z can be depicted as an annular region. It can be observed that when the adversary is unaware of a node's location, the possibility of pinpointing the location of an event is quite low. If the adversary is not a one-hop neighbor of the message source reporting the event, Z becomes very large.

5. Proposed scheme

A WSN is a self-organizing ad hoc network in which sensor nodes communicate over the shared medium through broadcast. A node can receive the public keys of its neighbors and can employ a self-organizing privacy scheme using ring signature. The notion of ring signature signifies anonymous signature generation without the revelation of the original signer. In a ring signature scheme, a set of potential signers are assigned. It does not require any coordinator or initiator as compared to group signature. The major difference between these two schemes is that the latter requires an entity called Group Manager which predefines a group of entities and distributes some secret keys to them. Ring signature does not require any such coordinator and rings can be formed autonomously, in a self-organized way. In a typical ring, all the nodes are equipped with a pair of public keys and private keys. Signer node produces a signature using its private key, the message itself, and all the other public keys of other nodes The formalization of the ring signature given is as follows.

Ring-Sign: *(m,*P_1*,*P_2*,....*P_r*,s,*S_s) With the public keys P_1,P_2,....P_r corresponding to r ring members, along with secret key S_s which is the *s*-th member (actual signer) produces a ring signature σ for the message *m*. The signer uses a probabilistic algorithm for the signature generation.

Ring-verify: (*m,* σ) The verifier accepts a message *m* and a signature σ including all the public keys of all the possible signers if it's true else reject it. Ring Signature Verification is a deterministic algorithm.

There are three basic security requirements for a ring signature scheme.

Signer Ambiguity: The probability that a verifier will be unable to determine the real signer of a ring with size *r*, is greater than *1/r*. Hence the anonymity in the ring signature is limited and can be computational or unconditional. When the verifier is a participator of the ring and not the actual signer, then it can guess the actual signer with a probability not greater than *1/(r-1).*

Correctness: When a signer generates a ring signature with any signature scheme correctly, the verifier satisfies the verification equation.

Unforgeability: Ring signature poses the strongest definition of unenforceability. Any non-ring member trying to forge a ring signature, on behalf of other ***n*** ring members, where he is not part of the message and being successful is negligible. So, members who are not part of the signature cannot forge any message.

From the property of the ring signature, it can be observed that the size of any ring signature grows linearly with the size of the ring, since the signature has to incorporate the list of ring members.

1) **Privacy of the Data:** The anonymous authentication scheme based on Each node *i* in the network is associated with a pseudonym which is the public key of the nodes working as authenticators as well as an identifier. Every Node *i* sensing the event belongs to a ring R_i which is a collection of finite nodes distributed over the network. Let $R = \{R1, R2, R3,.....\}$ be the set of rings formed in the network. After the occurrence of an event, the evolution of the rings takes place. Let m is the information related to an event and $N = \{N_1, N_2, N_3.....N_m\}$ be the neighbors where $m<S$, S = set of nodes deployed in the area. For each node $i \in N$, generates ring signature σ $(m, P1, P2,..., Pr, i, Si), P1, P_2,..., P_r$ public key of the nodes and S_i is the secret key of the node. The other nodes in the network upon receipt of (m, σ) verify the signature. If the received signature at node *i* contains P_i, then node **i** outputs true and forwards the message else discard it. The signer remains anonymous throughout the network. The sensed object or event is securely transferred to the sink through the nodes which are part of the evolved rings. Any entity which is not part of the ring cannot gain knowledge about the information in the message. So this scheme fulfills our goal of data privacy.

2) **Privacy of the Event:** Data is embedded into an encrypted message; also the message is transferred through the formation of a ring signature which helps the nodes to preserve their identity. The source of the message is the signer of the ring. The signer sends the message anonymously through the ring formation. Thus the identity of the signer is not revealed. In our assumed scenario, the signer of the ring is the node that senses the event or object. Since the signers are themselves anonymous, the location of the event remains undisclosed to non-ring members. This ensures contextual privacy in terms of the location of the event or object.

A. **Robustness of the Proposed Scheme:**

In this section, we will be discussing the expediency of our proposed scheme against different attack scenarios. First, its effectiveness against local adversaries will be analyzed followed by a more powerful kind of attackers called global adversaries.

1) **Against Local Adversaries:** There are few inherent properties of ring signature, whose occurrence in the network may favor adversaries to trace a node and tamper information. Two signatures generated by the same node are not equivalent, since the anonymity set are becoming different, so ring signatures are unlikable. Also, the signer S_i of a ring R_i is anonymous to an adversary, only if the adversary is unable to detect that *i* is the ring owner. If the public key of *i* is not used by any other ring in the network, in such scenarios an adversary can conclude that *i* is the owner of the ring R_i with a very high probability. This is a probable situation where node *i* can be compromised by the local adversaries. The probability that the public key P_S of signer S_I of the ring will not be used by any other ring is negligible. So, a local adversary close to the message source will not gain much information. Nodes form the ring based on the event generated in the network, so there will be redundant paths to the sink from the source. The redundant path may have node *i* such that $i \in R_m$ and $i \in R_n$ where R_m and R_n are two different ring anonymity sets. An adversary trying to eavesdrop on the network will be interested in more traffic flow zone. The nodes near the sink will have more traffic. As mentioned earlier, each node in the network will be part of some ring. So near the sink, there will be more nodes belonging to more than one anonymity set. Such nodes will be the target of an adversary to learn about the information flow in the network. The compromised node in such a case may give a false positive or false negative response and will send a message

to the next hop. Since the compromised node will be part of some ring, the downstream nodes in the anonymity set can detect the adversary action.

2) **Against Global Adversaries:** Global adversaries are assumed to have more computational and communication power. It can have more information than the local adversaries about the network, like the ring formation pattern, location of more traffic flow. It can also make the local adversaries collude. Global adversaries can locate redundant paths, by observing the traffic pattern. We have discussed how a node can be compromised by the local adversaries and the detection of such compromised nodes. We assume that Global adversaries will be interested to know about the event that occurred in the network. The adversary sitting in a node common to different rings will try to correlate the outputs, thus gaining access to one of the upstream nodes. So global adversaries can make a correlation attack. This can compromise very nodes and tamper with the sensed data. But there are multiple paths in the network to report the event to the sink. The probability of compromising all of them is very low. So sink or the other downstream nodes will receive multiple values from different paths. This will make the downstream nodes conclude that an attack has occurred in the network and thus the event is also compromised.

6. Simulation and results

Numerous simulation runs have been performed to validate the proposed scheme for resource-constrained sensor networks. Results obtained from these simulations are quite promising and show that our scheme performs quite well under different network scenarios.

Table 1. Simulation environment parameters

Parameters	Value
Network area	100x100 square meter
Number of nodes	Variable(10 to 100)
Bandwidth	250Kbps
Physical layer model	Log-normal shadowing
MAC protocol	TMAC
Routing Protocol	Multipath rings routing
Simulation time	3600s
Transmission power	57.42mW
Radio model	CC2420
Initial energy	18720 Joule (2AA battery)
Application layer packet size	Variable (2Kb to 4Kb)

For different simulations, we have changed node density, ring size, etc and it has been found that using ring signature to achieve privacy is quite a robust scheme and satisfies the basic needs of scalability, energy consumption in terms of the wireless sensor network. In this section, the validity of this scheme will be shown through simulation results incorporated in graphs.

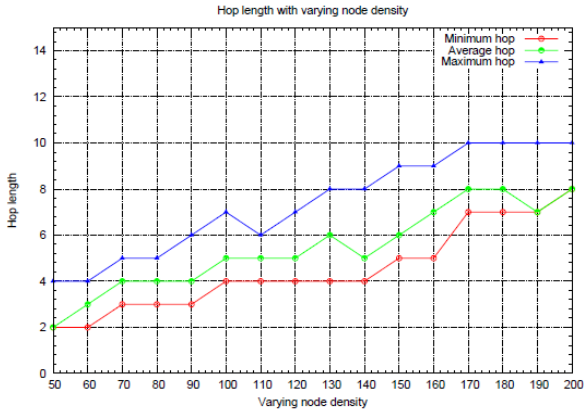

Figure 2. Hop counts vs node density

In Figure 2, the minimum hops, average hops, and maximum hops from random sources to sink are shown for varying node density with ring size 3. It is visible from the graph that as the node density increases, the number of hops increases linearly, except for non-linearity at some points. This happens for all cases of minimum, average and maximum hops.

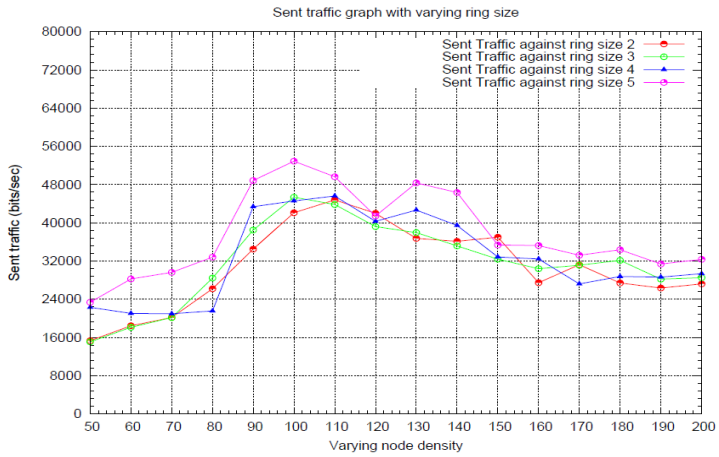

Figure 3. Hop counts vs node density

Figure 3, gives the information about the sent traffic for the different ring sizes. The traffic flow in the network increases with an increase in the number of nodes. It is also observed that the traffic becomes steady as the number of nodes increases from 150. With 120 nodes, there is a dip, this is due to the random event generation behaviour. As the ring size increases, the overhead in the network increases, and hence the traffic increases. Similarly, [Figure 4], shows the received traffic for varying ring size and node density.

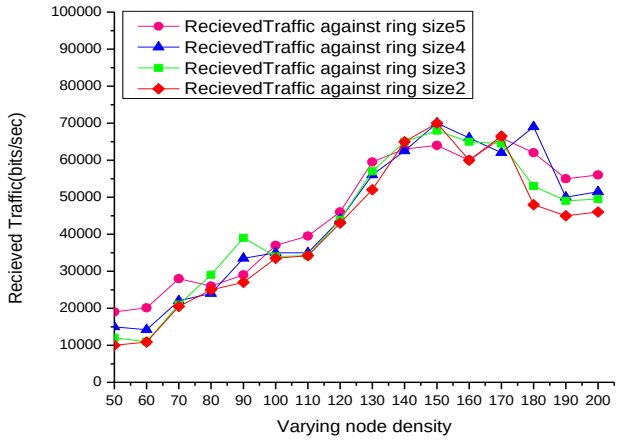

Figure 4. Received traffic vs node density

The sent traffic as well as received traffic Statistics for varying ring size and node density are captured from MAC Layer. The sent traffic corresponds to the average traffic sent by the nodes for varying simulations. The received traffic corresponds to the traffic received at the sink. Apparently, from the received traffic graph, we say that as the overhead in the network increases due to the increase in the ring size, the received traffic at the sink also increases.

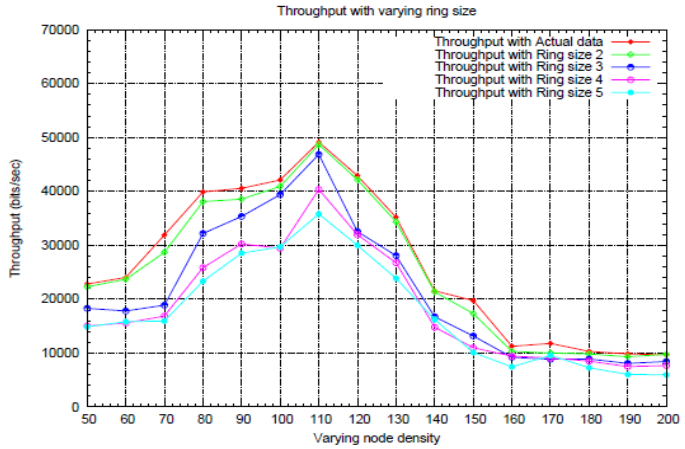

Figure 5. Throughput with raw and actual data

[Figure 5]. This shows the throughput of the network under the proposed scheme is analyzed. Throughout the network is analyzed for both raw and actual data. The actual data corresponds to the data being transferred, without the cryptographic overhead. We consider raw data to be the data with cryptographic overhead. The comparative graph shows that the throughput with raw data is close to the throughput with actual data. This shows that the cryptographic overhead does not tamper with the performance of the network.

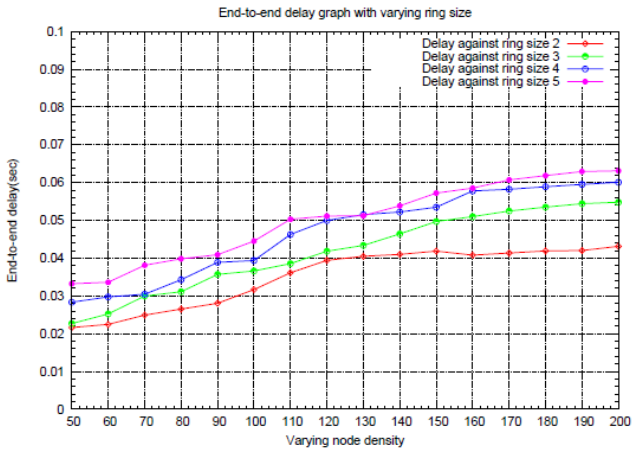

Figure 6. End –to end delay vs node density

[Figure 6]. Gives the end-to-end delay in the network, under the proposed scheme. The cryptographic schemes introduce queuing delay and processing delay in the network. Overall, the delay in the network is linear with the increased number of nodes. The delay is almost steady for nodes greater than 150. This behavior is almost similar to the throughput. Hence, we conclude, end-to-end delay at the application level will not vary too much with the increase in node density and ring size, which largely satisfies our need and promises to ease the burden on the whole network.

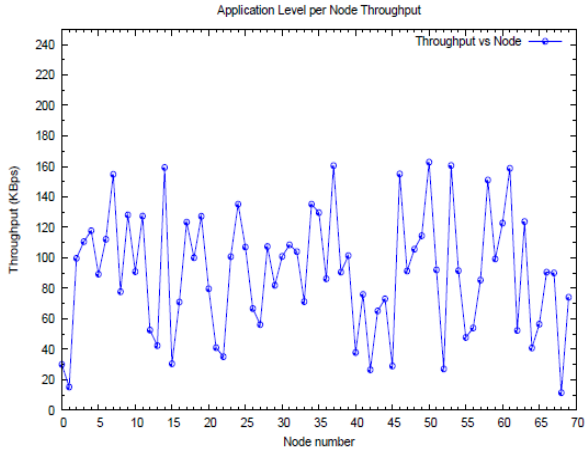

Figure 7. Throughput per node

The per-node throughput and latency for 70 nodes deployed in a 100X100 meter area with ring size 3 are shown in Figure 7 and Figure. 8 respectively for simulation of 7200s. From the figures, we observe that the maximum throughput of a node is 160KBps and the minimum is found to be 10 kbps.

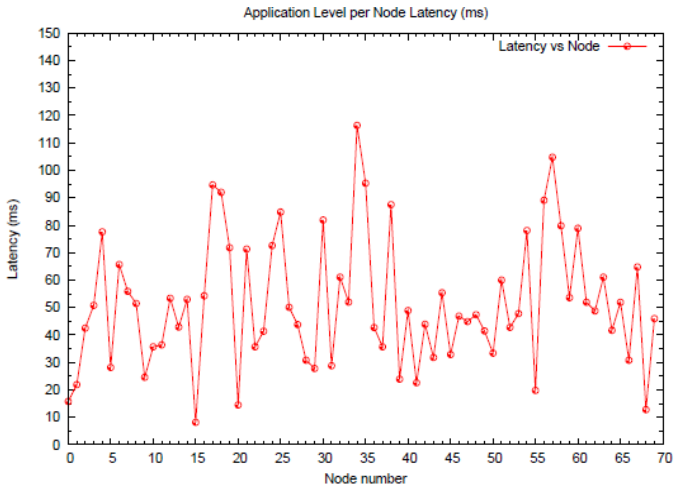

Figure 8. Latency per node

From [Figure 8, the maximum per node latency is found to be 120 ms. The minimum latency is approx 6ms. We note that the throughput is maximized when the latency is minimized for a node. The application-level per node latency and throughput show the efficacy of the scheme. The cryptographic overhead will consume more power for the encryption and decryption process. So, we have analyzed the energy consumed per node and thereby calculated the expected lifetime of the network under the proposed scheme.

In Figure 9, we have plotted the energy consumed by each node for simulation with 70 nodes. From the graph, we see that the maximum energy consumed per node is 6.6 Joule whereas the minimum energy consumed is 1.5 Joule, for the simulation time of 3600s. The nodes which become part of the ring signature consume more energy compared to other nodes, due to the signature generation and verification overhead. The energy consumed per node increases when the node gets associated with more rings. In figure 10 expected lifetime has been shown by varying numbers of nodes deployed against without using any cryptographic scheme and using ring signature scheme. Computation overhead is an inherent problem with any cryptographic scheme, which works as an impediment for the maximum of the schemes. The main challenge with the implementation of any cryptographic scheme is the energy efficiency as lots of energy is consumed for cryptographic key exchange, different digest calculations, etc. Our challenge was to see how well the ring signature scheme works in terms of energy consumption. We have taken the approach of measuring the expected lifetime to show the validity of our scheme in the face of energy consumption. We have assumed a network would be dysfunctional when 10% of the nodes die due to the lack of any other concrete paradigm of network lifetime. We can see network lifetime with a ring signature is quite close to a life without any cryptographic overhead. This proves that our proposed scheme can overcome the inherent overhead of cryptographic schemes.

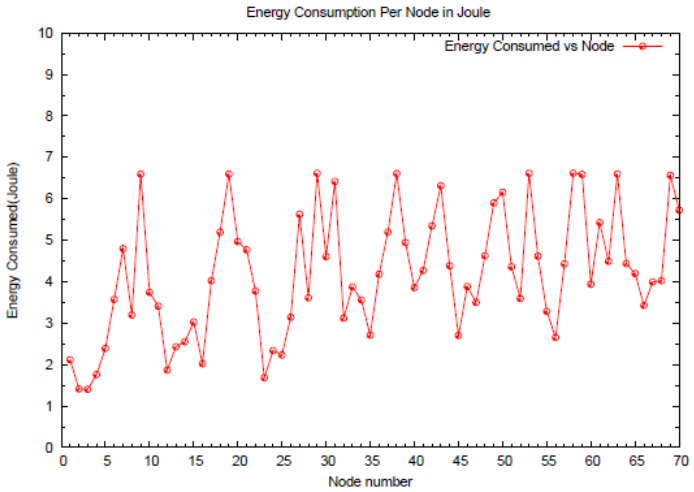

Figure 9. Energy consumed per node

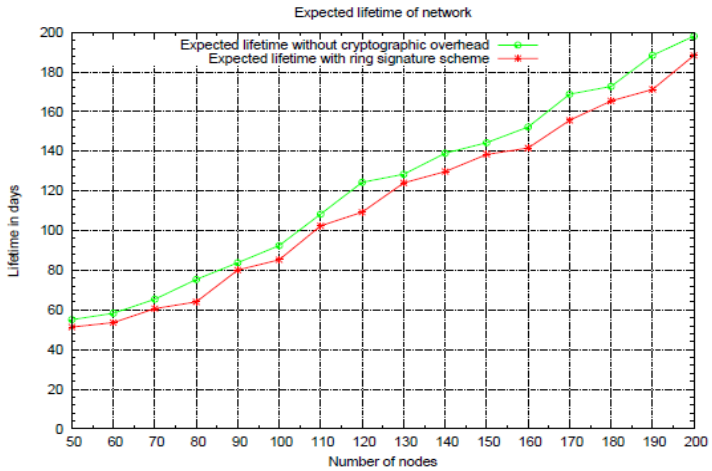

Figure 10. Expected lifetime vs node density

Preventing an adversary from learning the precise location of a sensed object or event can be accomplished by increasing the region of uncertainty using cryptographic or non-cryptographic mechanisms. Ring signature allows a sensor node to hide in the crowd of other signers of the ring. Ring signature gives unconditional anonymity to the signing sensor node together with authentication of the signer. This confirms the occurrence of the event of interest. We showed that the signers in the ring signature must be chosen from one-hop neighbors of the signing node. The number of signers in the ring needs to be more than three to prevent intersection attacks from global adversaries or adversaries near the sink where different routing paths congregate. The size and computational needs of the ring signature conflict with the resource needs of the sensor nodes and the throughput of the network. Moreover, the signing and verification delay become important in delay intolerant or actuator networks. To determine the efficacy of the proposed scheme, we performed a simulation-based study of the wireless sensor network. We observed that the computational requirements for generating and verifying the signature are well within the capabilities of nodes. The computation delay and end-to-end

latency due to the signature overhead are tolerable when compared to a raw network. Finally, we also found that the optimal number of signers was around three to four to prevent intersection attacks at points where most of the routing paths merge and preserve the privacy of a sensed object.

7. Conclusion

In this paper, we have proposed a scheme that assures to ensures both data and context privacy in the wireless sensor network. Ring signature with a lightweight signature scheme is used to ensure the privacy of the sensor nodes and privacy of the event location. With the use of our scheme, the network performance is found to be desirable. The lifetime of the network does not vary much with the life without using any cryptographic scheme. We also found that the privacy attack depends on the ring size formed in the network. The network is secure against correlation attacks when the ring members are more clustered which means the nodes belong to the same rings. Through various simulation results, we have shown that the problem of redundant paths has been mitigated with our scheme as the hop count is quite less. Finally, we can conclude this self-organized privacy-preserving scheme is lightweight enough to be used in wireless sensor networks.

References

[1] N. Li, N. Zhang, SK. Das and B. Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey", Ad Hoc Networks, vol. 7, no. 8, **(2009)**, pp. 1501-1514.

[2] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing", Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS), **(2005)** June 6-10; Columbus, Ohio, USA.

[3] P. Kamat, W. Xu, W. Trappe, and Y. Zhang, "Temporal privacy in wireless sensor networks", Proceedings of the 27th International Conference on Distributed Computing Systems (ICDCS), **(2007)** June 25-29; Toronto, Ontario, Canada.

[4] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks", Proceedings of the 20th International Parallel and Distributed Processing Symposium (IPDPS), **(2006)** April 25-29; Rhodes Island, Greece.

[5] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar and G. Cao, "Towards event source unobservability with minimum network traffic in sensor networks", Proceedings of the First ACM Conference on Wireless Network Security (WiSec), **(2008)** March 31 - April 2; Alexandria, Virginia, USA.

[6] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper", Proceedings of the IEEE International Conference on Network Protocols (ICNP), **(2007)** October 16-19; Beijing, China.

[7] R. Lu, X. Lin, H. Zhu, and X. Shen, "TESP2: Timed Efficient Source Privacy Preservation Scheme for Wireless Sensor Networks", IEEE Conference on Communication (ICC), **(2010)** May 3-10; Cape Town, South Africa.

[8] I. J. de Dieu, J. Wang, D. J. Asturias, S. Lee, and Y. Lee, "EDPPS: An Energy-efficient Data Privacy Protection Scheme for Wireless Sensor Networks", 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), **(2010)** October 27-30; Gyeonggi-do, Korea.

[9] Z. Qi, G. Yang, X. Ren, and Y. Li, "An ID-based ring sign cryption scheme for wireless sensor networks", IET International Conference on Wireless Sensor Network (IET-WSN), **(2010)** November 15-17; Beijing, China.

[10] R. Zhang, Y. Zhang and K. Ren, "DP²AC: Distributed Privacy-Preserving Access Control in Sensor Networks", INFOCOM, IEEE, **(2009)** April 19-25; Rio de Janeiro.

[11] Y. Li and J. Ren, "Preserving Source-Location Privacy in Wireless Sensor Networks", Sensor, Mesh and Ad Hoc Communications and Networks (SECON '09), 6th Annual IEEE Communications Society Conference on, **(2009)** June 22-26; Rome, Italy

[12] O. Cheikhrouhou, A. Kouba, O. Gaddour, G. Dini and M. Abid, "RiSeG: A logical ring based secure group communication protocol for Wireless Sensor Networks", Communication in Wireless Environments and Ubiquitous Systems: New Challenges (ICWUS), International Conference on, **(2010)** October 8-10; Sousse, Tunisia

[13] R. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret", Advances in Cryptology, 7th International Conference on the Theory and Application of Cryptology and Information Security, **(2001)** December 9-13; Australia

[14] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups", Proceedings of CRYPTO'02, Lecture Notes in Computer Science, Berlin: Springer-Verlag, vol. 2442, **(2002)** August 18-22; Santa Barbara, California, USA

[15] J. Xiao and G. Zeng, "Improved threshold ring signature for ad-hoc group", International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), **(2006)** September 22-24; Wuhan, China

[16] L. Wang, G. Zhang and C. Ma, "A survey of ring signature", Frontiers of Electrical and Electronic Engineering in China 2008, vol. 3, no. 1, **(2008)**, pp. 10-19

[17] J. Freudiger, "Evolution of Self Organized Privacy", EPFL, **(2008)**