



King Saud University
**Journal of King Saud University –
Computer and Information Sciences**

www.ksu.edu.sa
www.sciencedirect.com



FULL LENGTH ARTICLE

Privacy in wireless sensor networks using ring signature

Ashmita Debnath, Pradheepkumar Singaravelu *, Shekhar Verma

Indian Institute of Information Technology, Allahabad, India

Received 10 June 2012; revised 8 February 2013; accepted 21 December 2013

KEYWORDS

Privacy;
Security;
Wireless sensor network;
Ring signature;
Authentication

Abstract The veracity of a message from a sensor node must be verified in order to avoid a false reaction by the sink. This verification requires the authentication of the source node. The authentication process must also preserve the privacy such that the node and the sensed object are not endangered. In this work, a ring signature was proposed to authenticate the source node while preserving its spatial privacy. However, other nodes as signers and their numbers must be chosen to preclude the possibility of a traffic analysis attack by an adversary. The spatial uncertainty increases with the number of signers but requires larger memory size and communication overhead. This requirement can breach the privacy of the sensed object. To determine the effectiveness of the proposed scheme, the location estimate of a sensor node by an adversary and enhancement in the location uncertainty with a ring signature was evaluated. Using simulation studies, the ring signature was estimated to require approximately four members from the same neighbor region of the source node to sustain the privacy of the node. Furthermore, the ring signature was also determined to have a small overhead and not to adversely affect the performance of the sensor network.

© 2014 Production and hosting by Elsevier B.V. on behalf of King Saud University.

1. Introduction

Nodes in a wireless sensor network (WSN) observe their environment and send their observations to the sink (Mahmoud and Xuemin, 2012). The sensor data are characterized by their critical nature and spatial significance. The data sensed by a sensor node need to be sent to the base station via a secure communication channel. Networks can be either event-driven or time-driven. Whenever a message is

propagated through the network to the sink in an event-driven network, message authentication is imperative both in terms of data origin and content. Authentication (Daojing et al., 2011) helps to verify whether the source information has been tampered with or if a node has masqueraded as the source node and sent its own version of the message. Adversaries in the network can monitor the broadcast (Yang et al., 2011) by sensor nodes. These adversaries can obtain the time of an event based on the communication patterns, location of events and nodes from the message flow and see the unencrypted contents of the messages.

Using these methods, 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. This process compromises the security and privacy of the

* Corresponding author. Tel.: +91 9717952288.
E-mail addresses: rs64@iitaa.ac.in (A. Debnath), spradheepkumar@gmail.com (P. Singaravelu), sverma@iitaa.ac.in (S. Verma).
Peer review under responsibility of King Saud University.



network and most importantly the sensed object. This compromise may be used in a malicious manner. For example (Chow et al., 2011), poachers may track an animal moving in a forest by breaching both the spatial and temporal privacy of the sensed animal by monitoring the messages in the network. To protect the privacy of the sensed object, the spatial information from the messages along with temporal information that yield the time of occurrence of events must be cloaked (Chan and Perrig, 2003).

In WSN, sensor nodes are deployed in a region that is in close proximity 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. During transmission, the message payload that contains 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 contains information of the topology and current communication in the network. An adversary can eavesdrop on communication, read the clear text header information and obtain the identity of the source. However, we assume that the adversary 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. In a WSN, nodes are densely deployed, and an event usually occurs in the sensing regions of multiple nodes. Therefore, multiple nodes report an event. The adversary receives the broadcasts, examines the clear text header information to obtain the authentication information and source identity. Traffic analysis yields the approximate location of the nodes and sensed event. The mapping of the node identities with their location information can breach the privacy of the nodes and thus, the privacy of the sensed event. Therefore, the problem consists of obfuscating this mapping by hiding the node identities without hindering the authentication process. In this work, we concentrated on a mechanism to protect network's spatial context, such that the location of an event's occurrence cannot be garnered from the information available from messages or message flows. For example, in wild life monitoring, an adversary who can associate the time and place of origin of messages with the movement behavior of the animal can track a target animal. Thus, breaking the association of message flows from the location is imperative for sustaining the privacy of static or mobile sensed objects. Context-sensitive data can be secured in two ways: securing the location of sensor nodes and data sources or hiding the time at which an event is generated. To sustain the privacy (Jian et al., 2008) 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 de-correlating the data from the location and time of occurrence. In this study, we employed a ring signature to preserve the spatial privacy of the sensed object and nodes.

This privacy 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 2 describes the work related to the present study. The spatial privacy scheme is discussed and proposed in Sections 3 and 4 respectively. Section 5 contains the results with conclusion in Section 6.

2. Related work

Sensor networks feature two privacy concerns, data-oriented and context-oriented privacy. Data-oriented privacy (Jian et al., 2008) deals with securing the integrity of data gathered and transmitted to the destination. Context-oriented privacy (Tavli et al., 2010) prevents adversaries from gaining access to data context information, such as the time and location from which, the data originated. Data-oriented privacy focuses on proving protection to data items. Attackers can corrupt or eavesdrop on data to obtain critical information or inject false information in the network. A passive adversary eavesdrops (Kamat et al., 2005) on communication between nodes to determine the location of nodes or tracks the evolution of events. Cryptographic schemes can mitigate this type of unlawful behavior. 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 the location and time. The location can refer to the node location or data origin location. If an adversary can detect the location of a sink or the area, where an event has occurred, it can breach the privacy of information. It may also track (Kamat et al., 2007) or compromise a sensitive critical target.

The problem of privacy preservation (Alfantookh, 2006) is addressed by perturbing the parameters that are monitored. The underlying probability distributions are changed such that definite patterns cannot be constructed from the perturbed data and the relationships between different entities are uncorrelated. Increasing the entropy also increases privacy (Mehta et al., 2007) by enhancing the crowd size or the diversity. This enhancement can be achieved by employing cryptographic or non-cryptographic mechanisms. Various non-cryptographic mechanisms (Sabto and Al Mutib, 2013) have been studied in the literature. Random walk (Lu et al., 2013) has been used in Phantom routing (Li et al., 2012), and randomized routing (Al-Muhtadi, 2007) has been used along with flooding to hide the location of the source. Fake message injection (Li and Ren, 2009) and path perturbation algorithms (Rabai et al., 2013) 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 (Hu et al., 2007). Cryptographic techniques (Islam and Biswas, 2013) for privacy complement non-cryptographic techniques, such as routing, virtual ring creation, etc. The choice of cryptographic technique is important, as it consumes resources of the network. This consumption may adversely affect the latency, throughput and network lifetime. Many approaches provide the privacy of nodes and data; while ensuring efficient resource consumption. A new time efficient source privacy scheme, TESP2, against the traffic analysis attack of a global eavesdropper that can monitor and analyze the traffic in the entire network has been proposed (Chen et al., 2012). In TESP2, a sensor node broadcasts a request for timed data collection to its upstream nodes. Each upstream node sends the

163 cipher text of the real data or else sends the cipher text of the
164 dummy data if it lacks any real data. To preserve the source
165 privacy, the sensor node will discard any dummy data, re-en-
166 crypt and forward the cipher text of the real data to the down-
167 stream nodes.

168 3. Spatial privacy

169 We consider the sensors ($S = \{S_1, S_2, S_3, \dots, S_x\}$) to be de-
170 ployed where x is the population of the deployed sensors.
171 Nodes are assumed to be deployed in a uniform random distri-
172 bution. Prior to deployment, each sensor is assumed to be
173 loaded with a public/private key pair (P_i, S_i) for ($i = 1, 2, 3,$
174 $4, \dots, x$). Among the available public key cryptosystems, we as-
175 sume the use of ID-based public key cryptography. Local
176 adversaries and global adversaries exist. The local adversary
177 has limited access to the network information and can monitor
178 traffic from its one-hop neighbors. Unlike the local adversary,
179 the global adversary can contain information related to the en-
180 tire network. It has the capability to monitor the entire net-
181 work as well as access the local adversary. Local adversaries
182 can also collude and provide information to the global
183 adversaries.

184 3.1. Location uncertainty

185 In WSN, nodes are randomly scattered over a specific area
186 such that each point in the region is within the sensing range
187 of at least one node. The locations of the nodes in this random
188 network follow a spatial stochastic distribution. This arrange-
189 ment is usually taken to be a homogenous Poisson point pro-
190 cess of density (λ), and the number of nodes in any set A of
191 Lebesgue measure ($|X|$) is Poisson with mean ($\lambda|X|$). However,
192 when the number of nodes deployed in a region is fixed, the
193 Poisson point process is not a good representation of the node
194 distribution. The model may give more nodes than actually
195 present, especially when the number of nodes is small. When
196 a fixed and finite (say N) number of nodes are independent
197 and identically distributed in a region, the point process is
198 binomial. When (N) points in a compact set (W) are distrib-
199 uted independently and uniformly, the process is a binomial
200 point process. For any subset ($X \subset W$), the number of points
201 in (X) is binomial (n, p) with parameters ($n = N$) and
202 ($p = |X \cap W|/|W|$). The occurrence of event of interest or
203 sensed object that lies in the sensing region of sensor nodes
204 triggers communication from these nodes. A message emanat-
205 ing from a source node report on an event is heard by adver-
206 saries within the node's communication range. An individual
207 adversary or adversaries can collude to obtain a rough esti-
208 mate of the location of the sensed object. This estimated zone
209 (Z) is the anonymity zone. The level of anonymity of a sensed
210 object or event is the inability of the adversary to pinpoint its
211 location in the anonymity zone (Z). The degree of anonymity
212 of the sensed event is a function of the location uncertainty of
213 the sensor node reporting the event. This degree of anonymity
214 is in turn proportional to the area of the anonymity zone
215 ($A(Z)$). If (p_i) is the probability that the event occurs at a given
216 point in (Z), then ($\sum_{i=1}^p$). The entropy (Yu and Guan, 2008) of
217 the distribution of the anonymity set is
218 ($H(p) = -\sum_{i=1}^{A(Z)} p_i \log_2 p_i$). The anonymity of a given event is

219 maximized when all points are equally likely to be the potential
220 point of occurrence of the event of interest. Under this uniform
221 distribution, the probability (p_i) that a point (Z) under obser-
222 vation is the target becomes ($p_i \propto \frac{1}{A(Z)} A(Z) \subset W$).

223 Following the definition of the level of the anonymity given
224 in Yu and Guan (2008), we have, ($A_i = 1 - 1/|A(Z)|$) with en-
225 tropy ($H(p) = -\log_2 A(Z)$). The entropy of the anonymity set
226 is the measure of the privacy of a sensed object or event. If the
227 events form a binomial point process, then the events of inter-
228 est would be binomially distributed in the area ($A(Z)$).

229 The probability (p_z^k) that (k) events of interest of the point
230 process occur in the region (Z) is defined as the probability of
231 (k) points being in an arbitrary set (Z). If (N) nodes are distrib-
232 uted over a set (W), then ($p_z^k = \binom{N}{k} \frac{|A(Z) \cap W|^k}{|W|^k} (1 - \frac{|A(Z) \cap W|}{|W|})^{N-k}$).

233 In WSN, an event of interest may be observed by more than
234 one sensor node. An adversary in the network may be aware
235 of the node deployment or may not be aware of the node loca-
236 tions. A deployment-unaware adversary gauges the location of
237 the nodes from the signals broadcast by the nodes. A deploy-
238 ment-aware adversary knows the locations of the sensor nodes.

239 3.1.1. Case I: The adversary is deployment aware

240 3.1.1.1. The source is known. A sensor node observes an event
241 and transmits a message to report the event to the sink. The
242 broadcast is received by an adversary, who is in the communi-
243 cation range (R_c) of the sensor node. The adversary receives
244 the message and reads the contents of the clear text header
245 to find the source of the communication. The event of interest
246 must lie in the sensing range (R_s) of this source sensor node. To
247 ensure communication connectivity ($R_c \geq 2R_s$), the location of
248 the event must be within a circular region centered at the sen-
249 sor node with radius (R_s). This range is the anonymity zone (Z)
250 for the event. The event of interest would be located in the union
251 of sensing range of all the sensor nodes in (Z). Hence, its
252 privacy is proportional to the number of nodes that are in
253 (Z). The adversary who has heard the broadcast is sure that
254 at least one node is present in (Z), which is shown in Fig. 1.
255 The probability that (k) more nodes are present (where k is
256 determined by the level of desired anonymity) can be deter-
257 mined using Bayes' theorem as follows.

258 3.1.1.2. Source is not known. If the adversary cannot determine
259 the source of the message, then the anonymity zone (Z) be-
260 comes the union of the sensed region of the possible source
261 nodes and is larger than the first case. For example, the ano-

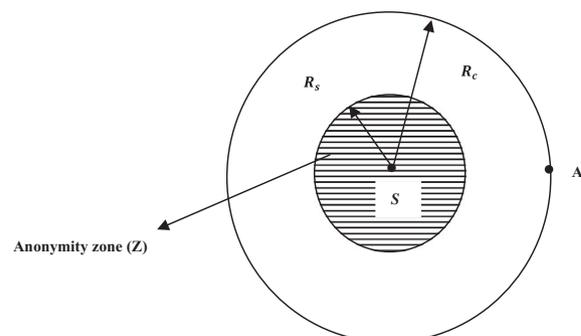


Figure 1 Anonymity zone (Z) (location of source is known).

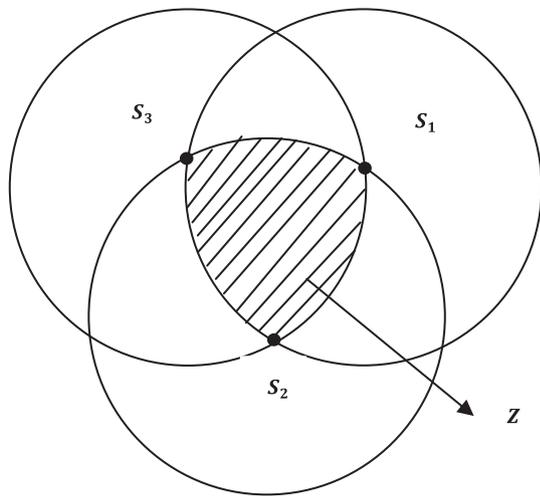


Figure 2 Anonymity zone (Z) (location of source is unknown).

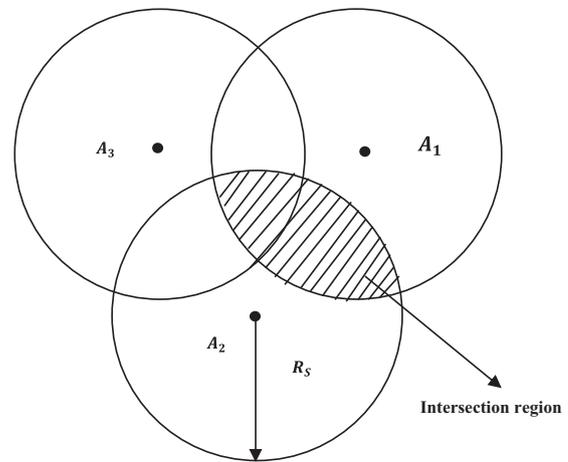


Figure 3 Interaction attack.

262 nymity zone (Z) for two neighboring sensor nodes is shown in
263 Fig. 2. (Z) is larger than in the first case. Thus, hiding the iden-
264 tity of sensor node reporting the event can increase the privacy
265 of an event of interest.

266 3.1.1.3. *Intersection attack.* The source does not know the
267 source of a message. However, multiple sensor report events
268 that occur in their vicinity by transmitting packets to the sink
269 over the network. These packets are routed toward the sink by
270 different nodes in the network. As the packets reach near the
271 destination, the routing paths may merge.

272 An adversary sitting at a particular location in the network
273 may receive messages from multiple sources. The possibility in-
274 creases if the adversary is near the sink. Different adversaries
275 may also communicate with one another over some private
276 channels. The adversaries are aware of the location of nodes,
277 and the occurrence of an event of interest is reported without
278 any delay. This process may allow an intersection attack by an
279 adversary that receives messages on a merged path within a
280 small time interval or by adversaries colluding to exchange
281 such information, which is shown in Fig. 3. The intersection
282 attack reduces the region of uncertainty and allows an
283 adversary to confine the search for the event of interest to a
284 very narrow region.

285 3.1.2. *Case II: The adversary is unaware of the node deployment*

286 A sensor node observes an event and transmits a message to re-
287 port the event to the sink. The broadcast is received by an
288 adversary who is in the communication range (R_s) of the sensor
289 node. The adversary estimates the rough location of the sensor
290 node from the received signal strength. Due to the noise and
291 variation in the signal attenuation in wireless channel, the node
292 may lie in an annular region, as shown in Fig. 4. Because a node
293 can sense an event in a circular region of radius (R_s), the event
294 of interest can be depicted as an annular region. When the
295 adversary is unaware of a node's location, the possibility of pin-
296 pointing the location of an event is quite low. If the adversary is
297 not a one-hop neighbor of the message source reporting the
298 event, the uncertainty region becomes very large.

4. Proposed scheme

299 A WSN is a self-organizing ad hoc network in which sensor
300 nodes communicate over the shared medium via broadcast.
301 A node can receive the public keys of its neighbors and employ
302 a self-organizing privacy scheme by using a ring signature
303 (Tscha, 2009). A ring signature signifies an anonymous signa-
304 ture generation without the revelation of the original signer.
305 In a ring signature scheme, a set of potential signers is assigned.
306 This scheme does not require a coordinator or initiator, unlike
307 a group signature (Das et al., 2013). The major difference be-
308 tween these two schemes is that the later requires an entity
309 called group manager, which predefines a group of entities
310 and distributes some various secret keys to them. Ring signa-
311 ture does not require such a coordinator, and rings can be
312 formed autonomously, in a self-organized way. In a typical
313 ring, all nodes are equipped with a pair of public and private
314 keys. A signer node produces a signature by using its own pri-
315 vate key to message itself and all the other public keys of other
316 nodes. The formalization of ring signature given in Yu and
317 Guan (2008) and is defined as follows. 318

- 319 (a) *Ring-sign* ($m, P_1, P_2, \dots, P_{r,s}, S_s$): With the public keys
320 (P_1, P_2, \dots, P_r) corresponding to (r) ring members, along
321 with secret key (S_s) which is the s^{th} member (actual
322 signer) produces a ring signature (σ) for the message
323 (m). The signer uses a probabilistic algorithm for the sig-
324 nature generation.
- 325 (b) *Ring-verify*: (m, σ) The verifier accepts a message (m)
326 and a signature (σ) including all the public keys of all possi-
327 ble signers if they are true, otherwise, the verifier rejects the
328 message. Ring signature verification is a deterministic
329 algorithm, which has three basic security requirements.
- 330 (c) *Signer ambiguity*: The probability that a verifier will be
331 unable to determine the real signer of a ring with size
332 (r), is greater than $(\frac{1}{r})$. Hence the anonymity in the ring
333 signature is limited, and can be computational or uncon-
334 ditional. When the verifier is a participator of the ring
335 and not the actual signer, it can guess the actual signer
336 with a probability no greater than $(\frac{1}{r-1})$.

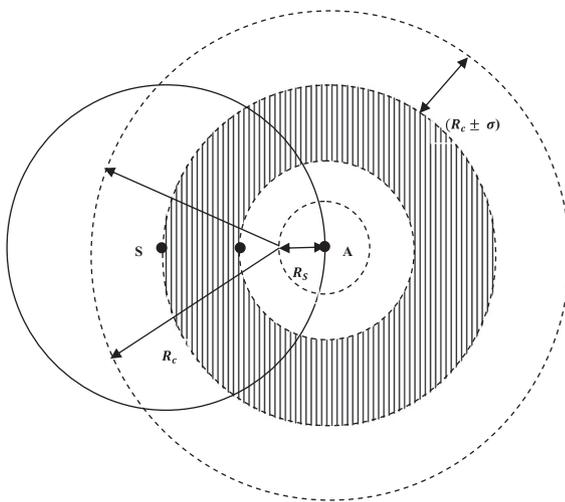


Figure 4 Anonymity zone (Z) (source location unknown).

- (d) *Correctness*: When a signer correctly generates a ring signature with any signature scheme, the verifier satisfies the verification equation.
- (e) *Unforgeability*: Ring signature poses the strongest definition of unforgeability. Any non-ring member trying to forge a ring signature, on behalf of other (n) ring members, for which the non-ring member is not part of the message and successful is negligible. Thus, members who are not part of the signature cannot forge any message. The property of the ring signature indicates, that the size of any ring signature grows linearly with the size of the ring, because the signature must incorporate the list of ring members.

(a) *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 authenticator 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 ($R = \{R_1, R_2, R_3, \dots, R_i\}$) be the set of rings formed in the network. After the occurrence of an event, the rings evolve. Let (m) be the information related to an event and ($N = \{N_1, N_2, N_3, \dots, N_m\}$) be the neighbors ($m < S$), where (S) as set of nodes deployed in the area. Each node ($i \in N$) generates as ring signature ($\sigma(m, P_1, P_2, \dots, P_r, i, S_i)$), where (P_1, P_2, \dots, P_r) are the public keys of the nodes and (S_i) is the secret key of the node. The other nodes in the network verify the signature upon receipt of (m, σ). If the received signature at node (i) contains (P_i), then node (i) outputs true and forward the message. Otherwise, the node discards it. The signer remains anonymous throughout the network. The sensed object or event is securely transferred to the sink through the nodes that are the part of the evolved rings. Any entity that is not part of the ring cannot gain knowledge about the information in the message. Thus, this scheme fulfills our goal of data privacy.

(b) *Privacy of the event*: Data are embedded into a message that is encrypted; moreover the message is transferred via 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. Because the signers are anonymous, the location of the event remains undisclosed to non-ring members. This scheme ensures the contextual privacy in terms of the location of the event or object.

4.1. Robustness of the proposed scheme

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

(a) *Against local adversaries*: Ring signatures contain few inherent properties that may favor adversaries to trace a node and tamper with information. Because the anonymity sets are different, two signatures generated by the same node are not equivalent. Thus, ring signatures are unlikable. Furthermore, 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, an adversary can conclude that (i) is the owner of the ring (R_i) with very high probability. This situation is problematic, where the local adversaries can compromise the node (i). The probability that any other ring will use the public key (P_i) of signer (S_i) of the ring is negligible. Thus, 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. Thus, redundant paths will lead to the sink from the source. The redundant path may contain 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 zones that contain more traffic flow. The nodes near the sink will have more traffic. As mentioned earlier, each node in the network will be part of some ring. Thus, more nodes belong to more than one anonymity set will be near the sink.

These nodes will be the targets of an adversary to learn about the information flow in the network. In this case, the compromised node may give a false positive or false negative response and will send message to the next hop. Because the compromised node will be part of some ring, the downstream nodes in the anonymity set can detect the adversary action.

(b) *Against global adversaries*: Global adversaries are assumed to have more computational and communication power. They can have more information than the local adversaries about the network, such as the ring formation pattern or location of more traffic flow. They can also make the local adversaries collude. Global adversaries can locate redundant paths; by observing the traffic pattern. We discussed how the local adversaries can compromise a node and the detection of such compromised nodes. We assume that global adversaries will be interested in events that occur in the network. The adversary sitting in a node common to different rings will attempt to correlate the outputs, thus gaining access to one of the upstream nodes. Thus, global adversaries can stage a correlation attack. This attack can compromise nodes and tamper the sensed data. However, multiple paths in the network report the event to the sink. The probability of compromising all of them is very low. Thus, the sink or the other downstream

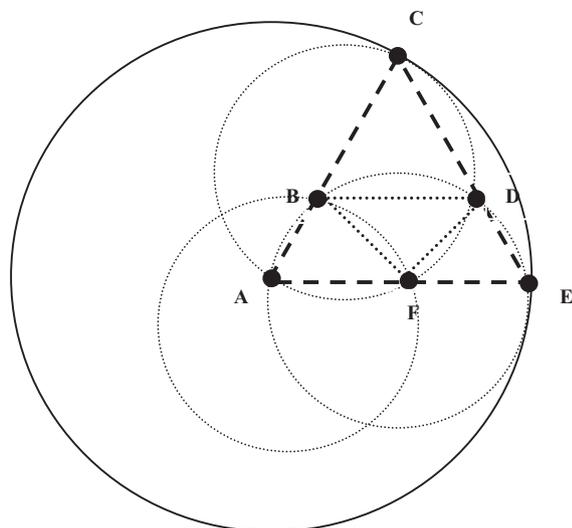


Figure 5 Maximum number of independent nodes connected to the sink node.

nodes will receive multiple values from different paths. This process will ensure that the downstream nodes conclude that an attack has occurred in the network and that the event has also been compromised.

In Fig. 5 of $G(V, E)$, where each node has the same transmission power, a node is adjacent to at most five independent nodes, which serve as its neighbor. Considering a small portion of a complete graph, node A will be surrounded by six dependent nodes; nodes B and F are two of them. Node B will dominate node A, node C, node F and node D. Similarly, node F will dominate node A, node E, node B and node D. The angle subtended at node A would be 60° . However, if this angle is increased by δ (say), then this symmetry will not hold; node B and node F will not remain connected. Hence, node A can be surrounded by a maximum of 5 independent nodes.

5. Simulation results

Several simulations runs were performed to validate the proposed scheme for resource-constrained sensor networks. The results obtained from these simulations are promising and demonstrate that our scheme performs well under different network scenarios. We changed the node density, ring size, etc, for each simulation and showed that using a ring signature to achieve privacy is a robust scheme and satisfies the basic needs of scalability and energy consumption in terms of WSN. In this section, the validity of this scheme will be demonstrated via simulation results that have been incorporated in graphs. Based on Fig. 6, the maximum per node latency was found to be 120 ms. The minimum latency is approximately 6 ms (Table 1).

We note that, the throughput is maximized when the latency is minimized for a node. The application level per node latency and throughput demonstrates the efficacy of the scheme. The cryptographic overhead will consume more power for the encryption and decryption process. Thus, we analyzed the energy consumed per node and thereby calculated the expected life time of the network under the proposed scheme. The per-node latency and throughput for 70 nodes deployed in a (100×100) meter area with ring size 3 is shown in Figs. 6

Table 1 Simulation environment parameters.

Parameters	Value
Network area	100×100^2 m
Number of nodes	Variable (0–70)
Bandwidth	250 kbps
Physical layer model	Log-normal shadowing
MAC protocol	TMAC
Routing protocol	Multipath rings routing
Simulation time	3600 s
Transmission power	57.42 mW
Radio model	CC2420
Initial energy	18,720 J (2AA battery)
Application layer packet size	Variable (2–4 kb)

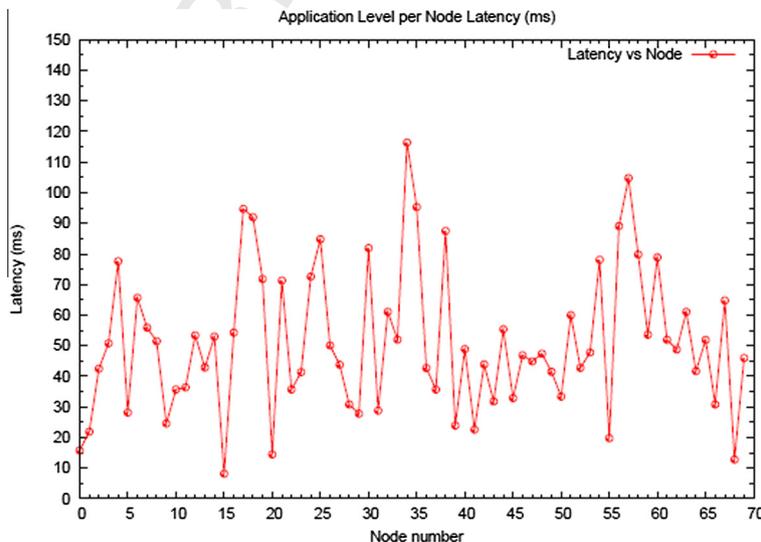


Figure 6 Latency per node.

475 and 7 respectively, for a simulation of 7200 s. The figures show
 476 that the maximum throughput of a node is 160 kbps, while the
 477 minimum was 10 kbps. In Fig. 8, we plotted the energy con-
 478 sumed by each node for a simulation with 70 nodes. The graph
 479 shows that the maximum energy consumed per node is 6.6
 480 joule, while the minimum energy consumed is 1.5 joule, for a
 481 simulation time of 3600 s. The nodes that become part of the
 482 ring signature consume more energy compared to other nodes;
 483 due to the signature generation and verification overhead. The
 484 energy consumed per node increases, when the node is associ-
 485 ated with an increased number of rings.

486 In Fig. 9, the expected lifetimes are shown by varying the
 487 number of nodes deployed against without using a crypto-
 488 graphic scheme and using a ring signature scheme. Computa-
 489 tion overhead is an inherent problem with any cryptographic
 490 scheme, which impedes the maximum of the schemes. The
 491 main challenge in the implementation of any cryptographic
 492 scheme is the energy efficiency, because a considerable amount
 493 of energy is consumed during cryptographic key exchange, dif-

ferent digest calculations, etc. We attempted to determine the
 energy efficiency of a ring signature scheme by measuring the
 expected lifetime in order to show the validity of our scheme
 in terms of energy consumption.

We assumed that a network would be dysfunctional when
 10% of the nodes die due to a lack of another concrete
 paradigm of the network lifetime. We can see that the network
 lifetime for the ring signature is quite close to the lifetime with-
 out any cryptographic overhead. This finding proves that our
 proposed scheme can overcome the inherent overhead of cryp-
 tographic schemes. The number of independent nodes in the
 vicinity of sink was only five. As the messages from a group
 of sensor nodes in a region move along different routing paths
 toward the sink, their paths overlap. This overlap makes the
 messages vulnerable to correlation attack. The adversary can
 find the ring members common to different messages and
 determine the original source node. Only two or three mes-
 sages overlap within a small time. If the ring members are from
 its own neighborhood and the numbers of signers exceed three,

494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512

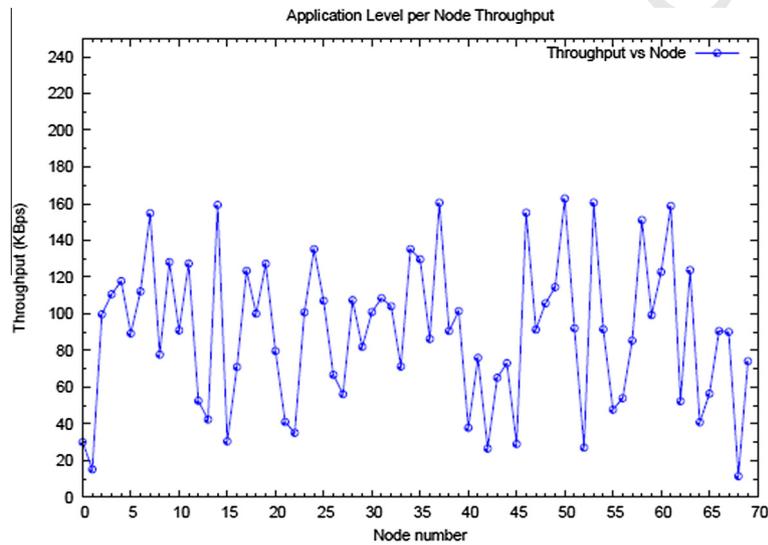


Figure 7 Throughput per node.

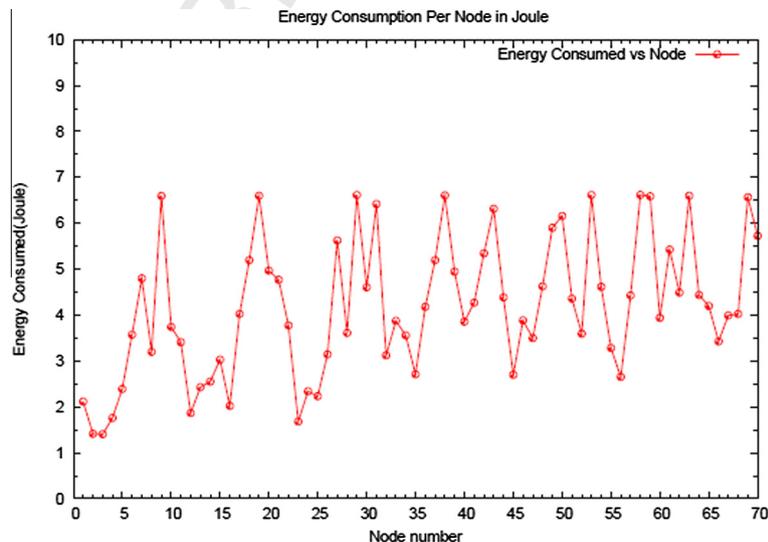


Figure 8 Energy consumed per node.

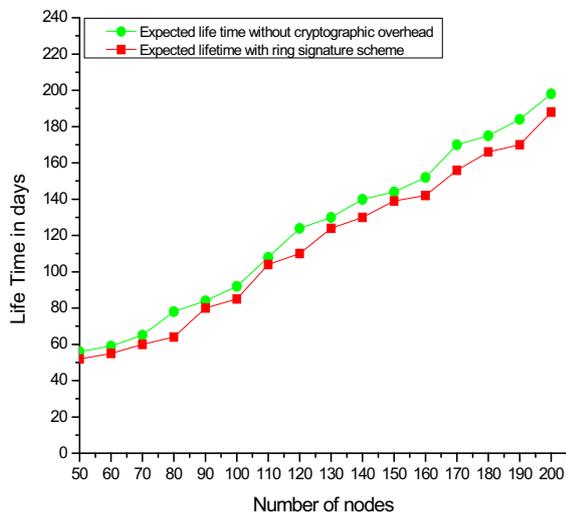


Figure 9 Expected lifetime vs. node density.

the correlation attack fails to provide a unique signer. Ring signature allows a sensor node to hide in the crowd of other signers of the ring.

Ring signature provides unconditional anonymity to the signing sensor node together with authentication of the signer. This scheme confirms the occurrence of the event of interest. We showed that the signers in the ring signature must be chosen from the one-hop neighbors of the signing node. The number of signers in the ring needs to exceed 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 WSN. 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 is tolerable when compared to a raw network. Finally, we also found that the optimal number of signers was near three to four; this number prevents intersection attacks at points where most of the routing paths merge and preserves the privacy of a sensed object.

6. Conclusion

An end user can be protected from taking a false action if the message originates from an authenticated source, whereas source nodes remain protected if the authentication technique preserves privacy. In a WSN, the traffic analysis and header information can reveal the location of a node. A ring signature-based authentication was proposed to preserve the privacy of a source node and obfuscate its residential region. The ring signature provides anonymity to the source, and the other members that are chosen from its neighborhood provide spatial anonymity. To balance the performance penalty due to the increased message size and vulnerability to interaction attacks by an adversary, the optimal number of signatures must

be near four, as suggested by the simulation experiments. The experiments also indicated that the scheme provided privacy and the performance penalty was negligible when optimal numbers of signers were used in the ring signature.

7. Uncited references

Xi et al. (2006) and Rios and Lopez (2011).

References

Mahmoud, M.M.E.A., Xuemin, S., 2012. A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* 23 (10), 1805–1818.

Daojing, H., Jiajun, B., Sencun, Z., Chan, S., Chun, C., 2011. Distributed access control with privacy support in wireless sensor networks. *IEEE Trans. Wireless Commun.* 10 (10), 3472–3481.

Yang, P., Cao, Z., Dong, X., Zia, T.A., 2011. An efficient privacy preserving data aggregation scheme with constant communication overheads for wireless sensor networks. *IEEE Commun. Lett.* 15 (11), 1205–1207.

Chow, C.Y., Mokbel, M.F., He, T., 2011. A privacy-preserving location monitoring system for wireless sensor networks. *IEEE Trans. Mob. Comput.* 10 (1), 94–107.

Chan, H., Perrig, A. 2003. Security and privacy in sensor networks, *IEEE Computer Magazine, USA*, pp. 103–105.

Jian, Y., Chen, S., Zhang, Z., Zhang, L., 2008. A novel scheme for protecting receiver's location privacy in wireless sensor networks. *IEEE Trans. Wireless Commun.* 7 (10), 3769–3779.

Tavli, B., Ozciloglu, M.M., Bicakci, K., 2010. Mitigation of compromising privacy by transmission range control in wireless sensor networks. *IEEE Commun. Lett.* 14 (12), 1104–1106.

Kamat, P., Zhang, Y.Y., Trappe, W., Ozturk, C. 2005. Enhancing source location privacy in sensor network routing, *Proceedings of the 25th IEEE International Conference on Distributed, Computing Systems*, pp. 599–608.

Kamat, P., Xu, W.Y., Trappe, W., Zhang, Y.Y. 2007. Temporal privacy in wireless sensor networks, *Proceedings of the 27th International Conference on Distributed, Computing Systems*, pp. 23–23.

Xi, Y., Schwiebert, L., Shi, W.S. 2006. Preserving source location privacy in monitoring based wireless sensor networks, *Proceedings of the 20th International Parallel and Distributed Processing Symposium*.

Alfantookh, A.A., 2006. DoS attacks intelligent detection using neural networks. *J. King Saud Univ. – Comput. Inf. Sci.* 18, 31–35.

Mehta, K., Liu, D.G., Wright, M. 2007. Location privacy in sensor networks against a global eavesdropper, *Proceedings of the IEEE International Conference on Network Protocols*, pp. 314–323.

Sabto, N.A., Al Mutib, Khalid, 2013. Autonomous mobile robot localization based on RSSI measurements using an RFID sensor and neural network BPANN. *J. King Saud Univ. – Comput. Inf. Sci.* 25 (2), 37–143.

Lu, R., Lin, X., Shen, X., 2013. SPOC: a secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency. *IEEE Trans. Parallel Distrib. Syst.* 24 (3), 614–624.

Li, Y., Ren, J., Wu, J., 2012. Quantitative measurement and design of source-location privacy schemes for wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* 23 (7), 1302–1311.

Al-Muhtadi, J., 2007. An efficient overlay infrastructure for privacy-preserving communication on the internet. *J. King Saud Univ. – Comput. Inf. Sci.* 19, 39–59.

Li, Y., Ren, J. 2009. Preserving source-location privacy in wireless sensor networks *Proceedings of the 6th Annual IEEE Communi-*

- 612 cations Society Conference on Sensor, Mesh and Ad Hoc 627
613 Communications and Networks, pp. 1–9. 628
- 614 Rabai, L.B.A., Jouini, M., Aissa, A.B., Mili, A., 2013. A cybersecurity 629
615 model in cloud computing environments. *J. King Saud Univ. –* 630
616 *Comput. Inf. Sci.* 25 (1), 63–75. 631
- 617 Hu, F., Jiang, M., Wagner, M., Dong, D.C., 2007. Privacy-preserving 632
618 telecardiology sensor networks: toward a low-cost portable wireless 633
619 hardware/software codesign. *IEEE Trans. Inf. Technol. Biomed.* 11 634
620 (6), 619–627. 635
- 621 Islam, S.K.H., Biswas, G.P., 2013. Provably secure certificateless 636
622 strong designated verifier signature scheme based on elliptic curve 637
623 bilinear pairings. *J. King Saud Univ. – Comput. Inf. Sci.* 25 (1), 51– 638
624 61. 639
- 625 Chen, C.M., Lin, Y.H., Lin, Y.C., Sun, H.M., 2012. RCDA: 640
626 recoverable concealed data aggregation for data integrity in
wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.* 23
(4), 727–734.
- Rios, R., Lopez, J., 2011. Analysis of location privacy solutions in
wireless sensor networks. *IET Commun.* 5 (17), 2518–2532.
- Tscha, Y., 2009. Routing for enhancing source-location privacy in
wireless sensor networks of multiple assets. *J. Commun. Netw.* 11
(6), 589–598.
- Das, A.K., Massand, A., Patil, S., 2013. A novel proxy signature
scheme based on user hierarchical access control policy. *J. King
Saud Univ. – Comput. Inf. Sci.* 25 (2), 219–228.
- Yu, Z., Guan, Y., 2008. A key management scheme using deployment
knowledge for wireless sensor networks. *IEEE Trans. Parallel
Distrib. Syst.* 19 (10), 1411–1425.

641

UNCORRECTED PROOF