I.J. Modern Education and Computer Science, **2014, 11, 58-66**
Published Online November 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2014.11.08

Enhanced Ring Signatures Schemes for Privacy Preservation in Wireless Sensor Networks

Sarthak Mishra
School of Computer Engineering, Kalinga Institute of Industrial Technology (KIIT), India
Email: saarthakmishra@gmail.com

Asst.Prof.Manjusha Pandey
School of Computer Engineering, Kalinga Institute of Industrial Technology (KIIT), India
Email: manjushapandey82@gmail.com

Abstract—Advancements in the domains of low-data-rate wireless networking and micro-electro-mechanical systems enabled the inception of a new networking domain, called wireless sensor network. These ad-hoc kind of networks have diversified applications in battlefield surveillance, disaster monitoring, intrusion detection etc. These networks consist plethora of sensor nodes which are severely resource constrained. As the application of the wireless sensor network is increasing, there is an emerging need for the security and privacy scheme which makes the network secure from various attacks and hide the ongoing activities in the network from a non-network entity. Privacy in wireless sensor network is yet a challenging domain to work on. Lot of work has been done to ensure privacy in the network. These relate to provide privacy in terms of the network entity and the privacy of the sensed information. Most of the solutions till date is based upon routing in the network layer, random walk based flooding, dummy data injection and cross layer solutions. Each of the schemes induce some overhead in the network. A light weight scheme is always desired for resource constraint wireless sensor networks. In this work we will propose a scheme which assures the privacy of the nodes in the network along with the privacy of the event generated in the network through a self organizing scheme. Through various simulation results the validity of our scheme among different network scenarios will be shown. We will also prove through graphical results that our proposed scheme enhances network lifetime quite satisfactorily.

Index Terms—Privacy, ring signatures, wireless sensor networks, cryptography, self-organizing.

I. Introduction

Wireless sensor networks have been the basis of large pool of applications in recent years. Advances in precise fabrication techniques and nano-technology enabled the evolution of tiny sensor nodes compared to its predecessors. In a typical wireless sensor network nodes sense the environment and delivers the data to a centralized entity. Along with the sensing unit nodes have onboard communication, data processing and storage system. Nodes are not only responsible for sensing and communication task, they are also capable of doing in network data processing, data fusion and correlation tasks.

A. Problem Definition:

In the field of wireless sensor networks various researches have been done to counter the distinct and challenging characteristics of its behaviour, mainly in the domains of MAC, Routing, Time-Synchronization, Data Aggregation etc. In spite of the importance of time and spatially important data, providing privacy has not been much researched domain. Ensuring privacy is not at all a less important objective in comparison to other domains in sensor networks, because of the role privacy plays in ensuring safe and secure communication. Applications where data gathered are critical both in terms of its time and spatial significance such as; volcano monitoring, earthquake monitoring, tsunami monitoring etc. Providing privacy to the data gathered, transmitted and processed at sensor nodes is an important task. Privacy is not only crucial in terms of content of data; it's also significant with respect to the context of data. Context of data can be visualized as the source of data, any event originating in the network, timestamp of data gathered etc. For example in habitat monitoring applications, data concerning association patterns of the animals can deter the objective of the application. Several potential challenges in sensor networks hamper the assurance of privacy. Some of these challenges are described below:

Uncontrollable environment: Sensors nodes are meant to be deployed in hostile and uncontrollable environments in a random fashion, sometime from airplanes or helicopters. One of such applications where nodes are deployed this way is battlefield surveillance. These types of applications are physical attack prone from adversaries. An adversary can physically damage a node or even distribute counterfeited ones. Either way violates the integrity of the network, and an adversary can easily gain access to the private keys. Resource constrains: Traditional private key algorithms and key distribution mechanism are inapplicable for wireless sensor nodes,

due to its severe resource limitations, mainly in terms of processing, memory and energy. This creates additional constraints to ensure privacy.

Topological constrains: Unique topological nature of wireless sensor networks makes them vulnerable to attacks on context-oriented privacy. Nodes closer to the sink node work as data forwarder to sink and they even generate and send their own data to the sink node. These nodes passes high amount of traffic. This kind of bizarre traffic pattern of sensor networks helps any adversary having the power of global traffic analysis to exploit the privacy of sink node or any node of significant interest. This hinders the basic objective of any sensor network.

A Data Oriented Privacy: Data oriented privacy focuses on proving protection to data items. By data items we not only mean the data collected but also the queries sent from outside authorities to the sensor network. Both data and queries can be corrupted by attackers to get critical information as well as injecting false information within the network. Two different kind of adversaries can affect data privacy; external and internal. An external adversary is one who sits outside of the network and tries to eavesdrop to data communication between any two nodes. This kind of unlawful behaviour can be mitigated by using traditional encryption schemes. Another kind of adversary is the internal adversary. These are the malicious nodes by antagonist entities; they can easily inject polluted information into the network through these nodes. In these kinds of attacks keys get compromised and so the very objective of providing privacy within the network. Research works done so far to ensure data-oriented privacy can be classified in two ways:

Privacy Protection during data aggregation: Data aggregation is the technique through which large volume of data can be compressed and fused to produce small amount of data that can eventually lead to lower traffic load in the network. This process works in a dual way in terms of privacy. External adversaries can be fooled by compressing data to a great extent and making it tough to compromise the integrity of data. Although the same process makes privacy vulnerable against internal adversaries.

Privacy of data Query: Securing the data queries sent to the network for obtaining results is a also a significant interest for the attackers. These queries can be tracked to check the activities happening inside the network and which zone is of much interest.

Most of the recent literatures concerning data privacy in wireless sensor networks are based on cryptographic techniques although primitive works on privacy mostly dealt with non-cryptographic techniques such as routing, virtual ring creation etc. Cryptographic techniques are important with respect to privacy in sensor networks, as they are light weight and largely affect the network lifetime. There are many generalized approaches to provide privacy of node and data in sensor network while ensuring efficient resource consumption.

1. TESP2: Timed Efficient Source Privacy Preservation Scheme for Wireless Sensor Networks
2. EDPPS: An Energy-efficient Data Privacy Protection Scheme for Wireless Sensor Networks
3. An ID-based ring sign encryption scheme for wireless sensor networks
4. DP2AC: Distributed Privacy-Preserving Access Control in Sensor Networks
5. Preserving Source-Location Privacy in Wireless Sensor Networks
6. RiSeG: A logical ring based secure group communication protocol for Wireless Sensor Networks

B. Context Oriented Privacy

The main focus of context oriented privacy is to ensure privacy of context related information such as location and time. Location can refer to node location or data origin locality. If an challenger can detect the spot of sink or the area where event occurred then it can easily attack the network. The attacker can potentially destroy the whole network or can even peak into the data transmitted by knowing the origin location. Ensuring timing privacy is another critical measure, concerning the time when data originated at the source node and when it reaches to the destination. If an attacker gets information of the time when these things happen in the network, then it can easily induce important information from the network. In a typical mobile target tracking application an adversary would try to get the time when the target passes through a particular zone and can infer significant knowledge to deduce the movement pattern. In case of context-oriented attacks there are two different types of attackers, local and global attackers. Local attackers can attack only a limited part of a sensing area. Whereas attackers with high antennas and other mechanisms called the global attackers can attack large portion of the network. Securing context-sensitive data can be done through two ways: securing location of crucial sensor nodes viz. data source or sink and securing the timestamp when important data are generated. There are many generalized approaches to provide context privacy of node and data in sensor network while ensuring efficient resource consumption.

1. Group Signature: In this fast moving technology, where many applications runs simultaneously by many users, there is always a requirement for the validation and authenticity of messages received, so that forged messages that seemingly appear to be valid, can be easily detected. Digital Signatures, which is a mathematical scheme for demonstrating the authenticity and validity of a message or a document, provides solution to such problems. A typical digital signature scheme consists of three algorithms: Key generation, A signing algorithm and a Verifying algorithm. So Digital signature does not procure the privacy of the signer and verifier, if they wish to keep the same.

There are many applications in the real life, where

privacy is required for signer and verifier. In such instances, additional work is required, to preserve the identity of the signer from the verifier. Group Signature provides solution to such applications. Group Signature uses the public key for verification of the signatures generated by group members which are also the signers. The verifier in the group can validate the signature without extracting the identity of the specific signer. The disadvantage of such schemes is that, group signatures require a setup phase of the group members hence not dynamic. Also the privacy of the group signature depends on the group manager, where the privacy of the signers can be revoked by the misbehaving signers using the extra trapdoor information stored with the group manager. The disadvantages of group signatures are resolved in ring signatures. The concept was first given by Rivest, Shamir and Tauman.

2. Ring Signatures are special type of group signatures without any trusted group managers which only have users and no managers. Group Signatures are used in applications where the group members agree to cooperate, where as ring signatures are used in applications where the group members are non-cooperative. Both group signature and ring signatures carry the property of signer ambiguity but the ring signature does not require prearranged group of users, no requirement for settings, changing and deleting group members, no requirement of distributing keys and most importantly , no way to revoke the identity of the actual signer, unless the signer himself decides to expose himself. Hence ring signature is said to improve the privacy preserving capability of group signatures by eliminating the requirement of a group manager and allowing signers to create group membership without the knowledge of the other members' identities and public keys.

II. Ring Signature and related study

Ring signature is the most flexible self-organizing scheme for ensuring privacy of the signers and verifiers. Typically any set of possible signers who may wish to sign is called a ring. In a ring signature, there is one signer who initiates the ring signature process. This actual signer is designated as signer of the ring. Other members of the ring who does not initiate the signing process are called non-signing members. The step by step procedure of any ring signature generation is mentioned below: Ring Sign**:** (m,P1,P2,....Pr,s,Ss) With the public keys P1,P2,....Pr corresponding to r ring members, along with secret key Ss which is the sth member (actual signer) produces a ring signature σ for the m message . The signer uses a algorithm in probabilistic approach 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 its true else reject it. Ring signature verification is a deterministic algorithm. The security requirements of ring signature are:

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 almost limited, and can be computed or may be unrestricted. When the verifier is a competitor of the ring and not the actual signer, then it can guess the actual signer with 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 enforceability. Any non-ring member trying to forge a ring signature, on behalf of other n ring members, where he himself is not part of the message and being successful is negligible. So members who are not part of the signature cannot forge any message.

A. Generation of Ring Signature

In the following section, the formal way of ring signature generation and verification procedures are discussed:

1. *Choosing a key*: The first step of ring signature generation is choosing a key. The role of the signer is to compute the symmetric key k which is defined as the hash of the message m to be signed:k = h(m) The more complicated version of k is computed as h(m,P1,....Pr). The security of the signature is enhanced with the more complicated hash functions. However, a simple hash is also secure as given above.
2. *Selection of random value:* After selection of hash function, the signer selects an initialization also called glue value *v* uniformly at random from *f0,1gb*.
3. *Pick Random xi's*: The signer has to select random values for its other ring members *1 < i < r, i6=s*, from *f0, 1gb* uniformly and independently; where r is the number of members in the ring, and computes *yi = gi(xi).*
4. *Solve for ys*: After this, the signer solves the ring equation for ys: Ck; v(y1; y2; :::yr) = v It is an assumption that, for any given arbitrary values for the other inputs, ys has a unique value to satisfy the equation which can be efficiently computed.
5. *Signer inverts the trap-door permutation:* The signer obtains xi, by using its knowledge of his trapdoor in order to invert *gi* on *yi : xs = gs^{-1}(ys)*
6. *Output of ring Signature:* The signature on the message m after signing process is defined by the *(2r +1) tuple: (P1; P2;:::Pr; v; x1; x2:::; xr)*

B. Verification of Ring Signature

After generation of the ring signature, it goes to the verifier. A verifier upon receiving the signature for the message *m* in the *(2r + 1)* tuple format (P1; P2;:::Pr; v; x1; x2:::; xr), does the following :

1. Verifier applies trap-door permutations: The verifier computes the following for all

i =1; 2; 3;:::::r yi = gi(xi)

2. Obtain the encryption key: To get the encryption key, the verifier hashes the received message m. *k = h(m).*

3. Verify the ring equation: After applying the trap-door permutations and obtaining the encryption key, the verifier finally checks that the ***yi***'s satisfy the fundamental equation. Ck;v(y1; y2; :::yr) = v.

If the above ring equation is satisfied then the signature is accepted as valid by the verifiers else its rejected. 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. It is an intrinsic shortcoming of ring signature as compared to group signatures with pre-defined group members. Typically, ring signatures are secure against adaptively chosen message attack in random oracle model. This is only violated, when a polynomial bounded forger has a positive advantage in the following case:

1. The Forger first chooses a signer that he or she is interested to compromise and corrupt. Using a challenger C, the forger tries to receive the partial private keys of the compromised signers.
2. The challenger C runs the setup algorithm with the security parameter k and shares the system parameter with the forger F.
3. Forger F performs hash function queries and signature queries polynomial number of times. Depending on the responses received from the challenger, the forger presents its queries adaptively.
4. After that the forger F outputs a valid signature.
5. The forger F outputs a signed message m, which is signed by a group of n signers. This signed message does not appear in the set of previous queries and the challenger returns less number of private keys. The forger only wins this game, when the signature turns out to be valid. The probability that the forger may win is the only advantage to him.

C. Categories of Ring Signature:

Ring signature has very flexible properties and thus it has gain wide popularity. Because of its group property, unconditional anonymity and spontaneity it is the most favourable self organizing privacy scheme used in most of the ad hoc based networks. Depending on the applications, ring signature till date has given different schemes. A ring signature has features of threshold property, link ability, anonymity revocation and deniability. Hence with different applications and accordance with the requirement features, a ring signature demands different features. So in the view of different schemes, ring signature can be classifies into four types:

1. *Threshold and general access ring signature:* Let A(t,n) is a threshold signature scheme. In A(t,n) signature scheme, t or more group members can generate the signature for the group. Valid signature generation would not be possible if a group has less than t members. Also any set of group members cannot impersonate another set of members to sign any message, not having any responsibilities. In case of any disputes, the threshold signature can be revoked or opened to detect the original signers without revealing the private keys. This feature of ring signature makes threshold based ring signature useful for companies to share a secret within the company. Bresson et al proposed threshold ring signature in 2002. He applied threshold signature scheme with ring signature and proposed a modified threshold ring signature. A t threshold signature signifies that not less than t members from a group have signed a message. Each ring signature is confirmed by at least t members that they have generated the message. The members of a set have the authority to choose any family of sets and prove to the access members that, they are cooperating members who have computed the signature, keeping the information about the set secret. Bresson et al utilized a combinatorial notion called fair partition to introduce a provably secure scheme.

2. *Linkable ring signature:* The concept of linkable ring signature was first introduced by Liu et al. This signature scheme gives the technique to determine, if two ring signatures are generated by same group member. In a new suitable reduction form of widely popular rewind simulation lemma which also satisfies the properties of anonymity. Based on the proposed scheme by Liu, a new efficient one-round e-voting system without any registration phase was constructed. Linkable ring signature scheme was later enhanced by Tsang et al , by introducing the security notions related to accusatory and non slander ability. The authors also presented first separable linkable ring signature scheme, which has the feature to support an efficient threshold option. In ref , a new linking criterion based on event generation was proposed called as event oriented link ability compared to group oriented link ability. In group oriented link ability, one can tell if two ring signatures are signed by same group, whereas in event oriented link ability one can determine if two ring signatures were created for the same event, even they were created on behalf of different group members. This shows that event oriented linkable signature schemes have more uses and are comparatively more flexible in real world applications. To capture practical and new attacking scenarios, Liu and Wong enhanced the previous security model by adapting more powerful notion of signer anonymity and redefining link ability.

3. *Verifiable ring signature:* A ring signature scheme makes the signer produce ring signature without disclosing its own identity. However, there can be cases, where the signer himself wants to disclose his identity to the verifier, or the verifier only wants to know the signer identity. There are many practical and real life examples for such cases. The ring signature generated by the signer requires being in identity disclosed manner. Suppose the Government issues a notification, that any person who can find the criminal or gives information about the most wanted person, can report to government. In such a case, government may receive messages containing useful information, but at the same time government needs to verify that it came from a valid person. Hence government needs to identity the signer of the message.

Also there will be many persons who will be sending information, and each one of them will be willing to claim to the verifier, here the government that, they have given information and claim the reward. Therefore there should be a mechanism in the ring signature that can disclose the identity of the actual signer only to the verifier. This feature designed and introduced by Lv and Wang in 2003 and formalized the notion of Verifiable ring signatures. So the verifiable ring signature poses the following extra properties: If the actual signer wants to prove that it has produced that signature to the recipient, then the receiver can check whether this claim is valid or not. Gan and Chen proposed an efficient way to transform the original ring signature scheme by Rivest into a verifiable ring signature scheme, in which actual signer can possibly embed its identity information into a subliminal channel. There are also ring signatures scheme posing all the properties of the Rivests signature scheme, but it also enables the original signer to convert the ring signature into ordinary signature through releasing few information. Such ring signature scheme is known as convertible ring signature scheme. Among most of the verifiable ring signature schemes, the identity of the actual signer can be publicly verified. However there are few verifiable signature schemes, where the designated verifier can only verify and identify the actual signer. The verifier cannot prove the identity of the signers to others, since in this case the verifier uses the zero knowledge proof with a non-transferability property.

4. Deniable ring signature: The ring signature scheme which has the property of anonymity revocation is known as deniable ring signatures. This was first proposed by Susilo and Nu. In this ring signature scheme, the verifier can interact with the signer or entities to confirm that the signer or entity has signed the signature with zero knowledge interactive proof. In this signature scheme, any signer cannot shift blame to other entities. Denial ring authentication is a combination of ring signatures and deniable authentication. Digital signatures provides authentication of messages thus providing non-repudiation of messages. In most of the applications, non-repudiation is one of the desirable properties, but in some applications it may not be. Inspired by such requirements Naor introduced Deniable ring signature scheme in 2002. In such ring authentication scheme, the verifier can be convinced that a entity of an ad-hoc group of participants is authenticating a message m, by not disclosing the identity information of the signer entity. It is also not possible for the verifier to convince any third party entity that message m is authenticated. This has been found in a number of applications. The Deniable ring signature scheme has the following properties:

1. It should be a good authentication scheme if no adversary can force a receiver to accept a message for which it is not the intended receiver. So it should be forgery resistant.
2. The authentication is done in way of zero knowledge sense, i,e the recipient may do simulated conversation and the result is indistinguishable.
3. The authentication does not reveal the identity of the source, i,e it preserves the anonymity in the group of sender, for any arbitrary set of users or any two members of the group and generate indistinguishable conversations to the recipient.
4. The scheme should not assume that, the verifier of the authentication process is part of the system and established a public key. Hence this section concludes the various types of ring signature existing till date.

D. Applications of Ring Signature

To appreciate the necessity of ring signature in practical real life applications, Lingling has cited practical scenarios viz leaking a secret or Designated Verifier. Since then, the applications of ring signature emerged in various fields and eventually became a powerful tool for applications in the field of military affairs, National secret Agency, Management, Politics, economics and the like. Ring signatures play a vital role in keeping the secret information, voting for the crucial leaders, e-commerce, press releasing and many more. The Applications of ring Signature is broadly classified as follows:

*Leaking Secrets***:** Ring Signature are used to disclose secrets in an anonymous way, where the identity of the person leaking the secret is hidden, still the verifier is convinced about the authenticity of the disclosed secret. E-Voting or e-cash system: Linkable ring signature scheme are useful for solving the problem of tracing the double spenders or voters directly. So this can be used in e-voting or e-cashing system directly. A short Linkable ring signature scheme is used for such applications especially when the size of the ring is large. Short linkable signature schemes works well to detect double spenders, although it does not work well for tracing the identity of the spender.

Ad-hoc Networks and wireless sensor networks: The rapid and steadily growing importance of digital portable devices and mobile applications has spawned various new types of groups and interacting parties which are now-a-days very popularly known as ad-hoc groups. ad-hoc group are highly dynamic in nature so it creates new challenges for net- working and its security. These kind of network have minimal infrastructure, without fixed routers or stable links. Spontaneous ad-hoc groups inherently work with these ad-hoc networks, other type of ad-hoc groups are independent of any network infrastructure. Example, A group of users spontaneously decide to communicate confidential data require a suite of protocols without any involvement of any third party or certification authorities with any new public keys. The security of such networks is re considered in the new context. The setup free property spontaneity property of ring signature makes it perfectly suitable for infrastructure less networks. In addition to ad-hoc networks, ring signature is of significant importance for Wireless sensor networks since its working is similar to ad-hoc-networks. This may solve many problems in wireless sensor networks like anonymous authentication

among the nodes in the network or providing privacy of a node or privacy of a event.

E. Ring Signature as a Privacy Preserving Scheme in WSNs

Traditional approach in security and privacy was designed to depend on central servers to protect the individual entity by obfuscating the identifying information. But there are several drawbacks in this approach. The most critical is the central server is the single point of failure which controls the private information of other devices. Second, when the users try to contact the central servers for anonymity, there is more traffic overhead in the network and more traffic create opportunities for the adversaries to analyse and attack if they intend to and can also be used to identify the users. Hence Self Organized privacy has become a novel paradigm to provide security and privacy in mobile networks. Self organized privacy does not require any co-ordinator or central servers to maintain privacy. Security and privacy is based on groups of the users themselves without the need of central authority.

In wireless sensor network, nodes often join into the network group and old members leave the group. Since the nodes are not constant and changes their dynamics with time, self organizing privacy without a manager or coordinator is an important aspect in sensor security. Both group Signatures and ring Signatures provide self organizing privacy. But group signature is manager dependent and works when group members are cooperating. Whereas ring signature do not require any group manager and group members can be non-cooperative which is exactly in correlation how sensor network works. Hence ring signature can be used as self-organized privacy scheme for wireless sensor network.

The security of the ring signature used in wireless sensor network also depends on how the rings are formed. The benefits of the ring signature are compromised if the ring members are not chosen properly. Suppose, a node belongs to only one ring in the network, i,e the public key information of the node is not used by any other ring in the network. It is a favourable condition of the adversary to find the ring owner and hence compromise that node. So the ring formation coordination must be maximized to achieve maximum anonymity to defend various adversary attacks. So the viability of using ring signature for providing anonymity and spontaneity for self organized privacy sustains for wireless sensor networks.

III. Problem Statement & Proposed Scheme

The scheme used here is based on self-organizing privacy scheme. This section gives the description about the sensors, respective public and private key pair model and event generation in the network. This is followed by the threat model of the network and the kind of adversaries which pose threat to the network. The design goals of the proposed scheme are also listed.

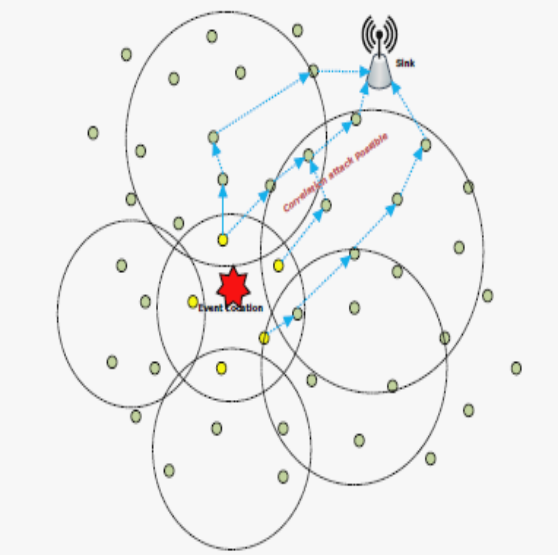

Figure 1. Network model with attack scenario

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. Prior to deployment, each sensor is assumed to be loaded with a public /private key pair ***(pi; si)***, for *i = 1; 2; 3; 4;.....x*. Among the public key cryptosystems available, we assume to used ID-based public key cryptography. The event generation in the network, is considered to be random. Event is sensed by the neighboring sensor nodes where the event has occurred. These neighboring nodes will try to report the event occurred to the sink or base station through anonymous authentication, maintaining the privacy of the event as well as privacy of the nodes in terms of location and identity. So the neighboring nodes of the occurred event will form a ring signature groups addressing other selective nodes in the network. The size of the rings will depend on the number of neighboring nodes when the event has occurred. The payload of the messages will depend on the number of nodes in the anonymity set of the rings thus varying the network performance. Fig 1 depicts the aforesaid scenario. The yellow color nodes are the neighbor nodes where the event has occurred. These nodes are the initiators of the ring. We assume that the nodes under the big circles are part of the anonymity set of the respective signers which is a yellow node. The sensing nodes report the event to the sink thus forming multipath. Near the sink there is a node, which is part of two rings. This can be threat for a correlation attack. We discuss this attack model relevant section.

2 Threat Model:

The adversary model is assumed to be both local adversaries and global adversaries. The local adversary will have limited access to the network information and will be able to monitor a small part of the network at any instance of time. An adversary may place eavesdropping

node in the network thus trying to deploy its own infrastructure. It can also exploit an existing infrastructure by accessing the network information. Unlike the local adversary, the global adversary is able to have information related to the whole network. Global adversaries are assumed to have more computational and communication power. It has the capability to monitor the whole network and access to local adversary as well. Local adversaries can also collude and give information to the global adversaries.

3 Design Goals:

Depending on the above model, the following design goals have been defined:

i. *Privacy of Nodes*: The nodes in the network should be able to authenticate themselves to the other nodes without being identified either by its location or node ID.
ii. *Privacy of the Event:* The location and the information related to a event generated in the network should be hidden while information is owing in the network from source to sink.

A. Proposed Scheme

This section discuss in detail about our two folded privacy preserving scheme for wireless sensor network using the self organizing privacy scheme of ring signature.

1. Privacy of Data:

The anonymous authentication feature based on ring signature is the key for achieving the objectives of the scheme. 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 identifier. Every Node i sensing the event belongs to a ring Ri 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 a event and *N = {n1,n2,n3.....nm}* be the neighbors where m < S, S = set of nodes deployed in the area. For each node i € N, generates ring signature σ(m; p1; p2;....; pr; i; Si) ,p1; p2;....; *pr* public key of the nodes and Si is the secret key of the node. The other nodes in the network upon receipt of *(m; σ)* verifies the signature. If the received signature at node i contains Pi, 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 the 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 fulfils our goal of data privacy.

2. Privacy of the Event:

Data is embedded into a message which is encrypted; also the message is transferred through the formation of ring signature which helps the nodes to preserve its 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 who senses the event or object. Since the signers are themselves anonymous, the location of the event remains undisclosed to non-ring members. This ensures the contextual privacy in terms of location of the event or object.

B. Solidarity of the Proposed Scheme

In this section we will be discussing about the expediency of our proposed scheme against different attack scenarios. First its effectiveness against local adversaries will be analyzed followed by 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 favors adversaries to trace a node and tamper information. Two signatures generated by the same node are not equivalent, since the anonymity set are becomes different, so ring signatures are unlikable. Also, the signer *Si* of a ring *Ri* 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 *Ri* with very high probability. This is a probable situation where the node i can be compromised by the local adversaries. The probability that the public key *Ps* of signer *Si* 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 in his favor.

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 € Rm and i € Rn where Rm and Rn 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 target of an adversary to learn about the information flow in the network. The compromised node in such case may give false positive or false negative response and will send 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 about 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 node can be compromised by the local adversaries and detection of such compromised nodes. We assume that

Global adversaries will be interested to know about the event occurrence 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 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 to conclude that an attack has been occurred in the network and thus the event is also compromised.

IV. Summary

The privacy preserving schemes proposed till date in wireless sensor network provides either data privacy or context privacy and in few schemes both the privacy schemes are proposed. Our scheme provides both data and context privacy with self organizing cryptographic technique. The distinguishing feature of this scheme is that, it provides self organized privacy with the potential to detect any compromised node as well as event in the network. This scheme is secure against local/internal adversaries and global/external adversaries.

V. Conclusions

In this paper we have proposed a scheme which assures to ensure both data and context privacy in wireless sensor network. Till now enormous amount of work have been carried out for achieving privacy in sensor networks. But maximum of these works concentrates on routing techniques. Although these techniques are quite robust against different adversary attacks, they incur significant overhead to the network. Problem with existing schemes is that in most of the cases too much redundant traffic flow is generated, which mars the objective of energy efficient design. Observing these problems, we proposed the scheme to achieve data and context privacy using ring signature. Network overhead in terms of less throughput and greater delay is an inherent problem with any cryptographic signature scheme. Reason behind this is the use of cryptographic keys, message digests and signature values.

We have proposed self-organizing privacy preserving scheme which uses light weight cryptographic scheme. Light weight source and message authentication is a critical for low delay reliable delivery of message in WSN. Ring signature scheme proposed in this work requires low computational power and reduced storage overheads due to the small key size and simple operations. As expected, the signature also results high throughput and less delay ratio. The queue build up at the nodes is also within their storage capacity. However, the key distribution and management has to be studied to establish the effectiveness of Ring signature for WSN.

References

[1] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, \Privacy preservation in wireless sensor networks: A state-of-the-art survey," Ad Hoc Netw., vol. 7, pp. 1501-1514, November 2009.

[2] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, \Enhancing source-location privacy in sensor network routing," in Distributed Computing Systems, 2005. ICDCS 2005. Proceedings.

[3] P. Kamat, W. Xu, W. Trappe, and Y. Zhang, \Temporal privacy in wireless sensor net-works," in Distributed Computing Systems, 2007. ICDCS '07. 27th International Conference on, p. 23, june 2007.

[4] Y. Xi, L. Schwiebert, and W. Shi, \Preserving source location privacy in monitoring-based wireless sensor networks," in Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International, p. 8 pp., April 2006.

[5] K. Mehta, D. Liu, and M. Wright, \Protecting location privacy in sensor networks against a global eavesdropper," Mobile Computing, IEEE Transactions on, vol. PP, no. 99, p. 1, 2011.

[6] R. Lu, X. Lin, H. Zhu, and X. Shen, \Tesp2: Timed efficient source privacy preservation scheme for wireless sensor networks," in Communications (ICC), 2010 IEEE International Conference on, pp. 1 6, may 2010.

[7] I. de Dieu, J. Wang, D. Asturias, S. Lee, and Y.-K. Lee, \Edpps: An energy-efficient data privacy protection scheme for wireless sensor networks," in Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on, pp. 451-456, 30 2010-dec. 2 2010.

[8] Z.-h. Qi, G. Yang, X.-y. Ren, and Y.-w. Li, \An id-based ring signcryption scheme for wireless sensor networks," in Wireless Sensor Network, 2010. IET-WSN. IET International Conference on, pp. 368- 373, nov. 2010.

[9] R. Zhang, Y. Zhang, and K. Ren, \Dp 000b2; ac: Distributed privacy-preserving access control in sensor networks," in INFOCOM 2009, IEEE, pp. 1251-1259, April 2009.

[10] P. Tsang, V. Wei, T. Chan, M. Au, J. Liu, and D. Wong, \Separable linkable threshold ring signatures," in Progress in Cryptology - INDOCRYPT 2004 (A. Canteaut and K. Viswanathan, eds.), vol. 3348 of Lecture Notes in Computer Science, pp. 337-376, Springer Berlin / Heidelberg, 2005.

[11] J. Liu, V. Wei, and D. Wong, \Linkable spontaneous anonymous group signature for ad-hoc groups," in Information Security and Privacy (H. Wang, J. Pieprzyk, and V. Varadharajan,eds.), vol. 3108 of Lecture Notes in Computer Science, pp. 325-335, Springer Berlin /Heidelberg, 2004.

[12] L. Wang, G. Zhang, and C. Ma, \A survey of ring signature," Frontiers of Electrical and Electronic Engineering in China, vol. 3, pp. 10- 19, 2008.

[13] J. Freudiger, \Evolution of self organized privacy," 2008.

[14] J. Liu and D. Wong, \Linkable ring signatures: Security models and new schemes," in Computational Science and Its Applications ICCSA 2005 (O. Gervasi, M. Gavrilova, V. Kumar, A. Lagan, H. Lee, Y. Mun, D. Taniar, and C. Tan, eds.), vol. 3481 of Lecture Notes in Computer Science, pp. 88-89, Springer Berlin / Heidelberg, 2005.

Authors' Profiles

Sarthak Mishra is currently pursuing M.Tech from Kalinga Institute of Industrial Technology in the School of Computer Engineering, Bhubaneswar. He has completed his B.Tech from Raajdhani Engineering College, Biju Patnaik University of Technology, and Bhubaneswar. His research interest areas include Wireless Sensor Network, Security and Privacy in Wireless Sensor Network and Computer Networks.

Manjusha Pandey is presently working as an Assistant Professor in the School of Computer Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar. She is pursuing her PhD from Indian Institute of Information Technology, Allahabad. She has more than 10 research publications to her credit in journals and conferences of repute. Her research interest areas include Wireless Sensor Network, Security and Privacy in Wireless Sensor Network, Human Computer.

How to cite this paper: Sarthak Mishra, Manjusha Pandey,"Enhanced Ring Signatures Schemes for Privacy Preservation in Wireless Sensor Networks", IJMECS, vol.6, no.11, pp.58-66, 2014.DOI: 10.5815/ijmecs.2014.11.08

