Scientific Journal Impact Factor (SJIF) : 3.518
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

DATA COMMUNICATION AND ACCESS CONTROL WITH SECURITY UNDER WSN

Ms. K. Ayesha.[1], Ms. V. Priya.[2], Ms.S.Suguna.[3], Ms. D.PonniSelvi.[4]
[1,3]Research Scholar ,[2,4]Asst. Professor,Department of Computer Science,
Vivekanandha College of Arts and Sciences for Women (Autonomous), Tiruchengode, Tamilnadu, India

Abstract - Sensor devices are deployed to monitor an area. Area surveillance is the main operation of the sensor devices. Radio frequency based data communication is adapted under the sensor network. Coverage property of the sensors is considered in the network deployment process.

Sensor network operations are handled between the network owner and the user objects. All the data access privileges are granted by the network owner with reference to the payment by the users. All the user request and response transactions are secured using the privacy preservation models. The sensor data access is managed with Distributed Privacy-Preserving Access Control (DP^2AC) scheme. Sensor data query process is verified with the tokens. The network owner verifies the tokens and transfers the query results to the user. Token preparation and verification operations are carried out using the blind signature values. Public verification and reuses control mechanism are supported by the Distributed Token Reuse Detection (DTRD) scheme. Witness nodes, Rectilinear Double Ruling and Spherical Double Ruling models are used for the token reusable detection process.

The secured data transmission scheme is integrated with the data verification methods. Digital signature based attack control mechanism is adapted in the system. The data query operations are protected with anonymous and malicious user attacks. Computational overhead and communication overhead are also minimized in the system.

Keywords: Wireless Sensor Networks, Blind Signature, Privilege Management, Token Generation and Verification and Privacy Preserved Data Query.

I. Introduction

Recent advances in microelectronic mechanical systems and wireless communication technologies have fostered the rapid development of networked embedded systems like wireless sensor networks (WSNs) [11]. WSN applications often need to be changed after deployment for a variety of reasons-reconfiguring a set of parameters, modifying tasks of individual nodes, and patching security holes. Many large-scale WSNs are deployed in environments where physically collecting previously deployed nodes is either very difficult or infeasible. Wireless reprogramming is a crucial technique to address such challenges.

Message authentication plays a key role in thwarting unauthorized and corrupted messages from being forwarded in networks to save the precious sensor energy. For this reason, many authentication schemes have been proposed in literature to provide message authenticity and integrity verification for wireless sensor networks (WSNs). These schemes can largely be divided into two categories: public-key based approaches and symmetric-key based approaches.

The symmetric-key based approach requires complex key management lacks of scalability and is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The shared key is used by the sender to generate a message authentication

code (MAC) for each transmitted message [1]. The authenticity and integrity of the message can only be verified by the node with the shared secret key is generally shared by a group of sensor nodes. An intruder can compromise the key by capturing a single sensor node. In addition, this method does not work in multicast networks.

II. Related Work

In this section, we first review some related work on privacy preserving techniques for participatory sensing, and then review the work on data aggregation. Finally, we analyze some key differences with the closely related previous work.

2.1 Privacy Preserving Techniques

In the current state-of-the-art, a number of privacy preserving techniques for participatory sensing systems, especially the location-based services (LBSs), have been proposed by previous researchers, mainly to address the privacy of data source identity, user location, user trajectory, and sensing data content itself. These techniques can be classified into the following four categories.

2.1.1 Randomization Based Techniques

Randomization based technique [9], where noise may be added into the original data, can hide the real value of sensitive information. This method was widely studied and used in data mining field. The loss of data quality is a significant shortcoming.

2.1.2 Generalization

The k-anonymity model, which aims to hide each user's sensitive information among k - 1 others', is a universal metric for privacy preservation, and has been applied to participatory sensing in several previous work. This kind of method usually needs an honest third-party as the anonymizer, which is not allowed in ubiquitous semi-honest models. Therefore, when a more severe situation of semi-honest third-party is considered, these approaches cannot meet requirements.

2.1.3 Cloaking Techniques

Cloaking techniques usually use generalization or perturbation to replace the actual location with larger area or to cloak real location using some functions. While spatial cloaking techniques can well protect single location information, they fail to protect the trace privacy, with which user's identity is also inferable [4]. Several work were proposed aiming to solve the trajectory privacy problems [3]. Same questions exist that the protection of privacy reduces the quality of reported data.

2.1.4 Cryptography Based Solutions

End-to-end encryption, which can guarantee the high security of reported data, is widely used for the privacy preservation [2]. Encryption can only protect participants' privacy from external attacks. When the encrypted data arrives at the service provider side, service provider can decrypt ciphertext and obtain the corresponding plaintext. Therefore, encryption technique fails to prevent the service provider from inferring users sensitive features. Since internal attacks are also undesirable, designing privacy preserving schemes for participatory sensing against both external and internal attacks are highly important.

2.2 Data Aggregation Protocols

Data aggregation is a widely used technique in wireless sensor networks. Data aggregation algorithms are designed to gather and aggregate data in an energy efficient manner so that the network lifetime is enhanced [6]. Cam et al. [7] presented a multi-stage real-time alert aggregation technique over mobile networks that greatly reduces the amount data transmission and attempts to maximize the bandwidth utilization. Kumar et al. [8] proposed a learning automata-based opportunistic data aggregation and forwarding scheme for alert generation in vehicle ad hoc networks (VANETs), which overcomes the challenges of high velocity and constant topological changes in VANETs and can

adaptively select the next hop for data forwarding and aggregation from the other nodes. Security issues are not considered in these data aggregation protocols.

As mentioned above, security is an important issue in the process of data aggregation. Secure data aggregation protocols achieve security requirements along with data aggregation. Aviv et al. [10] proposed a privacy-aware geographic message exchange protocol for Human Movement Networks (HumaNets). They only consider static networks. Therefore, these methods are not suitable for participatory sensing, where the network changes dynamically.

III. Privacy Ensured Data Query Process

Privacy ensured data query process in sensor networks has so far received little attention. Related work addresses access control by authenticating network users before granting them data access rights, but the privacy of users is not considered. As far as we know, SPYC is the only work that takes into account the access privacy of network users. SPYC assumes the first data acquisition method mentioned above, i.e., users acquire data through one or multiple base stations which may not exist in our target scenarios. It is thus a centralized solution orthogonal to our work in this paper.

DP^2AC is a Distributed Privacy-Preserving Access Control scheme for single-owner multiuser sensor networks. In DP^2AC, each user interested in sensed data purchases some tokens from the network owner before entering the sensor network, which can subsequently send a query with an unspent token to any sensor node. Once validating the token, the sensor node provides the user with an appropriate amount of requested data commensurate with the denomination of the token. Token generations involve blind signature, which leads to a desirable property: the validity of each token can be verified by any sensor node, but no one, including the network owner, can tell the identity of the token holder. The network owner can prevent unauthorized access to sensed data, while users can protect their data access privacy. DP^2AC is a nontrivial adaptation of untraceable electronic cash systems resource-poor sensor networks.

The system uses a suite of DTRD techniques and thoroughly compares their performance with regard to TRD capability, communication overhead, storage overhead, and attack resilience [5]. All these schemes rely on the collaboration of sensor nodes themselves without a single point of failure. Detailed performance evaluations confirm the efficacy and efficiency of the proposed DTRD techniques in thwarting token-reuse attempts, which makes DP^2AC a very practical and trustworthy solution for sensor networks.

IV. Problem Statement

The owner and users entities are involved in the sensor network communication. The network owner need enforce strict access control so that the sensed data are only accessible to users willing to pay. users wish to protect their respective data access patterns. Privacy preservation schemes are used to protect user data access information details. Distributed Privacy-Preserving Access Control (DP^2AC) scheme used in the sensor network. Tokens are issued by the network owner to the users for querying sensor data. Query responses are prepared and distributed after validating the tokens collected from the users. Blind signatures are created in token generation and used to publicly verify the public identity. A central component in DP^2AC is to prevent malicious users from reusing tokens. A distributed Token Reuse Detection (DTRD) scheme is used to validate tokens without involving the base station. Witness nodes are used to check the tokens are applied or not. Rectilinear Double Ruling and Spherical Double Ruling models are used for the token reusable detection process. The following issues are identified from the privacy preserved access control schemes in WSN.

- Data security is not provided

- Query response attack are not handled
- Computational overhead is high in token verification process
  Duplicate token verification is not performed

V. Distributed Privacy-Preserving Access Control

In this section, we outline the DP^{2}AC scheme and defer the details of token-reuse detection. DP^{2}AC involves three phases: the initialization phase where the network owner picks security parameters, the withdrawal phase where users purchase tokens, and the spending phase where users spend tokens for data access.

5.1. System Initialization

DP^{2}AC is based on Chaum's blind signature protocol which itself depends on RSA. The network owner creates its RSA public and private keys as <h,,n> and d, respectively. Here, n is the product of two distinct random primes p and q; e, $1 < e < \emptyset$, is coprime to $\emptyset = (p - 1)(q - 1)$; d, $1 < d < \emptyset$, satisfies $ed = 1 \bmod \emptyset$. The modulus *n* is typically at least 1,024 bits long for sufficient security. In DP^{2}AC, the public key <h,,n> is only used for verifying the network owner's signatures. To enable efficient signature verifications, we select e to be $2^{16} + 1$, which is commonly recommended in practice. The network owner publishes <h,,n> while keeping <p, q, d> confidential to himself. In particular, each sensor node is preloaded with <h,,n> prior to network deployment. The network owner later could use authenticated broadcast such as μTESLA update sensor nodes with a new public key whenever needed. In addition, we assume that each user can get an authentic copy of <h,,n>, e.g., from the network owner's website or a public-key certificate binding <h,,n> to the network owner which is issued by a trusted third party.

5.2. Token Withdrawal

Sensor network users need pre buy some tokens from the network owner. Each token in DP^{2}AC consists of a λ-bit random integer and the network owner's signature on it, where λ is a system parameter partially determining DP^{2}AC's correctness. Tokens can be purchased in many ways. The network owner is trusted to return a correct σ_m^*.We can see that σ_m is a valid RSA signature on h(m), as

$$\begin{aligned}\sigma_m &= k^{-1}\sigma_m^* \bmod n \\ &= k^{-1}h(m)^d k^{ed} \bmod n \\ &= k^{-1}h(m)^d k \bmod n \\ &= h(m)^d \bmod n.\end{aligned}$$

Due to the blinding factor k, the network owner cannot derive h(m) and σ_m from m*. In other words, given <m, σ_m>, the network owner cannot link it to Alice. Each token corresponds to a monetary value and can be used to purchase an appropriate amount of sensed data. It is also possible to enable multidenominational tokens by letting the network manager use a different RSA public/private key pair for each kind of denomination. For ease of presentation, we focus on single-denomination tokens throughput this paper. Although unable to precisely associate individual tokens with the identities of their holders, the network owner may still narrow down the holder of a particular token to the users who purchased tokens. This might be a concern if the number of token buyers is limited. To overcome this, users may depend on a trusted third party to purchase tokens, thus avoiding submitting payment information directly to the network owner.

5.3. Token Spending

The token-spending process is pretty simple. Consider Alice again as an example. After purchasing tokens, Alice can enter the sensor network to acquire data from any sensor node, say node A. Upon receiving a token <m, σ_m>, node A first checks if h(m) = $(\sigma_m)^e$ mod n holds, a standard RSA signature verification. The check should succeed for a genuine token because $(\sigma_m)^e$ = $h(m)^{de}$ = h(m) mod n. If so, node A runs the Token-Reuse Detection process to make sure that <m, σ_m> has not been used before. Only when <m, σ_m> passes both tests does A provide an appropriate amount of requested data to Alice that is commensurate with the token value. Since A cannot link <m, σ_m> to Alice, it does not know who requested the data as long as Alice does not disclose her identity. Alice's data access privacy is thus well protected. Also note that signature verification takes an average of 0.79 seconds on MICAz motes. So this operation is quite affordable in resource-constrained sensor networks.

5.4. Token-Reuse Detection (TRD)

Every token <m, σ_m> is simply a pair of numbers and unconditionally untraceable. Malicious users thus may unlimitedly reuse their tokens without worrying about being caught. It is therefore essential for sensor nodes to check whether received tokens have been used before answering data queries. This process is referred to as token-reuse detection hereafter, which is part of the token-spending phase and occurs right after a token passes the signature verification. The significant shortcomings of the centralized TRD approach which depends on the base station. We present a suite of distributed TRD schemes without involving the base station.

5.5. Rectilinear Double Ruling

There is a tradeoff between the TRD probability and the communication and storage costs: the larger β, the higher pr, the larger C_r and S_r, and vice versa. Scheme 1 is motivated by the double-ruling (DR) techniques for data dissemination and query in sensor networks, which can be viewed a variant of the quorum-based location update scheme to enable scalable routing in ad hoc wireless networks. The DR techniques aim at storing the sensed data along a continuous curve, called replication curve, instead of one or multiple isolated sensor nodes. Later users can query the data along another continuous curve, called query curve. As long as two curves intersect, users can retrieve the data of interest. In what follows, we introduce a TRD scheme built upon the simplest DR scheme, rectilinear DR. In the rectilinear DR technique, replication curves follow horizontal lines, while query curves follow vertical lines. If the sensor field has a regular topology, every replication curve will intersect with every query curve.

5.6. Spherical Double Ruling

We introduce another scheme to significantly reduce the communication cost of Scheme 1 while providing similar overwhelming TRD probability. Scheme 2 is a variation of the spherical double ruling scheme proposed is based on stereographic mapping. Assuming that the physical shape of the sensor field is known and regular, we can place a virtual sphere with radius l tangent to the sensor field at the origin which is also called the South Pole. Each point X in the sensor field can be mapped to a unique point X' on the sphere, which is the intersection of the line through X and the north pole with the sphere. Conversely, each point on the sphere can be mapped to a point on the sensor field except the North Pole if the sensor field is infinite. According to the property of stereographic mapping, every great circle on the sphere can be mapped to a circle in the sensor field, which we call projected circle. Intuitively, any two great circles on the sphere will intersect with each other at two points, so do any projected circles. Scheme 2 selects the replication/query curves as random projected circles, which are guaranteed to intersect with each other.

5.7. Bloom-Filter for Token Update Process

We extend our DTRD schemes to cope with unlimited number of tokens. In the previous DTRD schemes, each node directly records every token it receives in its buffer. One potential problem might be some sensor nodes' buffers may overflow if too many tokens are stored. To prevent this from happening, the network owner must equip each sensor node with sufficient memory to accommodate the maximum possible number of tokens, which is certainly not cost effective. Now we introduce a solution for this issue by replacing sensor node buffer with a bloom filter. A Bloom filter is a space-efficient data structure for representing a set T = $\{t_i\}_{i=1}^{w}$ by a φ bit vector to support membership checking.

VI. Secured Data Query Process and Privilege Management

The DP^{2}AC mechanism is improved with data security techniques. The query response attacks are using digital signatures. A counter based token verification model is used to reduce the computation overhead. The system verifies token attacks and query attacks. Payment based data sensing scheme is designed with security and privacy schemes. Distributed token verification is performed in the system. Query request and response values are protected with attacks. The system is divided into six major modules. They are network owner, token management, query authentication, witness node, token analyzer and response security. Network owner module is designed to handle the network deployment tasks. Users' registration and token issue operations are carried out in token management module. The query authentication module is designed to verify the query and token values. Witness node module is designed to maintain the used token details. Token analyzer module is used to verify duplicate tokens and malicious attacks. Response security module protects the query results with confidentiality and integrity.

The network owner manages the sensor nodes and network users. Sensor node placement is performed by the network owner. Sensor nodes are maintained with its coverage and node type details. Network owner is placed under the base station. Network user registration is designed to register new users for data monitoring. Tokens are issued with reference to the sensor node for data access. Payments for tokens are decided by the network owner. Token purchase process is invoked by the network users.

Network user issues the query value to the sensor nodes. The query values are enclosed with the tokens. Token authentication is performed to validate user query values. Query responses are prepared and transferred to the requested network user. The witness nodes are assigned by the network owner. Used token details are updated in the witness node. Sensor node verifies the query tokens using the witness nodes. Witness node checks the reusability of query tokens. The token analyzer module is used check the duplicate tokens. Malicious user request are also handled by the token analyzer. Counter values are used to update the token usage details. Tokens are verified with signature values. Sensor node sent response to the network user with reference to the query value. The RSA algorithm is used to protect response data security. The secure hashing algorithm (SHA) is used for the data integrity analysis. Response failures and attacks are also handled by the system.

VII. Conclusion and Future Work

The wireless sensor network is constructed by an owner to provide data for users. Data access operations are performed with reference to the advance payment tokens. Distributed Privacy-Preserving Access Control (DP^{2}AC) mechanism is used to perform access control with tokens. The system integrates the security and privacy model for the token and query response data values. The system combines security and privacy operations. Query responses are also protected from attacks. Efficient energy management model is supported by the system. Decentralized token verification system ensures the privacy and security for query request and response. The system can be enhanced with following

features. The data query system can be enhanced to support data caching scheme for fast data retrieval. The query system can be improved with privacy ensured data transfer model. The sensor network query scheme can be integrated with data sensing scheduling schemes. Centralized data owner based model can be upgraded to handle decentralized data owner model.

References

[1] Jian Li, Yun Li, Jian Ren and Jie Wu, "Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 5, May 2014

[2] J. Shi, R. Zhang, Y. Liu, and Y. Zhang, "PriSense: Privacy-preserving data aggregation in people-centric urban sensing systems," presented at the 29th IEEE Int. Conf. Comput. Commun., San Diego, CA, USA, Mar. 2010.

[3] D. Christin, J. Guillemet, A. Reinhardt, M. Hollick, and S. S. Kanhere, "Privacy-preserving collaborative path hiding for participatory sensing applications," presented at the 8th IEEE Int. Conf. Mobile Ad-hoc Sen. Syst., Valencia, Spain, Oct. 2011.

[4] H. Zang and J. Bolot, "Anonymization of location data does not work: Alarge-scale measurement study," presented at the 17th Annu. Int. Conf. Mobile Comput. Netw., Las Vegas, NV, USA, Sep. 2011.

[5] Rui Zhang, Yanchao Zhang and Kui Ren, "Distributed Privacy-Preserving Access Control in Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, August 2012.

[6] L. Mottola and G. P. Picco, "MUSTER: Adaptive energy-aware multisink routing in wireless sensor networks," IEEE Trans. Mobile Comput., vol. 10, no. 12, pp. 1694–1709, Oct. 2011.

[7] H. Cam, P. A. Mouallem and R. E. Pino, "Alert data aggregation and transmission prioritization over mobile networks," Netw. Sci. Cybersecurity, Adv. Inf. Secur., 2014.

[8] N. Kumar, N. Chilamkurti and J. J. Rodrigues, "Learning automata- based opportunistic data aggregation and forwarding scheme for alert generation in vehicular ad hoc networks," Comput. Commun., vol. 39, pp. 22–32, 2014.

[9] F. Zhang, L. He, W. He, and X. Liu, "Data perturbation with statedependent noise for participatory sensing," presented at the 31st Annual IEEE Int. Conf. Comput. Commun., Orlando, FL, USA, Mar. 2012.

[10] A. J. Aviv, M. Blaze, M. Sherr and J. M. Smith, "Privacy-aware message exchanges for HumaNets," Comput. Commun., vol. 49, pp. 30–43, 2014.

[11] Wei Dong, Yunhao Liu, Zhiwei Zhao, Xue Liu Chun Chen and Jiajun Bu, "Link Quality Aware Code Dissemination in Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 7, July 2014

