ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE International Journal of Advanced Research in Management, Architecture, Technology and Engineering
(IJARMATE) Vol. 3, Special Issue 11, March 2017

A FRAME WORK: SECURE DATA AGGREGATION IN WIRELESS SENSOR NETWORKS USING HOMOMORPHIC ENCRYPTION

V.BINDU [1], DR.NITHYA.M [2],

Research Scholar, V.M.K.V.Engineering College, Salem [1]
HOD – CSE, V.M.K.V.Engineering College, Salem [2]

Abstract—Communication in wireless sensor networks uses the majority of a sensor's limited energy. Using aggregation in wireless sensor network reduces the overall communication cost. Security in wireless sensor networks entails many different challenges. Traditional end-to-end security is not suitable for use with in-network aggregation. A corrupted sensor has access to the data and can falsify results. Additively homomorphic encryption allows for aggregation of encrypted values, with the result being the same as the result when unencrypted data was aggregated. Using public key cryptography, digital signatures can be used to achieve integrity. We propose a new digital signature algorithm which is based on the Elliptic Curve Digital Signature Algorithm (ECDSA) using homomorphic encryption and additive digital signatures to achieve confidentiality, integrity and availability for network aggregation in wireless sensor networks.

I. INTRODUCTION

Wireless sensor networks (WSNs) have permeated numerous applications, and are increasingly being relied upon for many mission-critical services like volcanic monitoring, forest fires monitoring, battlefield surveillance, agriculture monitoring, and railroad tunnels. In all these missions, hundreds or even thousands of sensors, self-organize themselves into a network for sensing, processing and transmitting information via multi-hop to a remote server (called a base-station). While a spectrum of research topics have garnered the attention of the WSNs community in the past, two of the most critical are lifetime and security.

Security in WSNs can manifest in many forms like authentication, confidentiality, integrity, reliability and availability. In many missions, it is likely that sensors and their readings are corrupted due to environmental factors such as water, wind or sand acting on the sensor & sensors may deliberately be corrupted by an attacker. Such corrupted sensors may appear to participate in the mission of the network, but may falsify sensor readings, improperly apply aggregation functions, exclude legitimate messages from the aggregate result or create fictitious results.

Homomorphic encryption schemes are one possibility of ensuring secure aggregation, as they allow data aggregation to be performed on encrypted data. Encryption and decryption operations are computationally very expensive and time consuming. In homomorphic encryption certain aggregation functions such as sum and average can be calculated on the encrypted data, reducing the workload of the sensors in the network significantly. The data is encrypted and sent toward the base station, while sensors along the path apply the aggregation function on the encrypted data. The base station receives the encrypted aggregate result and decrypts it. Homomorphic encryption schemes provide security against eavesdroppers and protect the aggregate result from being known by intermediate. Integrity of the aggregate result can easily be achieved on a hop-by-hop basis in wireless sensor networks. Achieving end to-end integrity while allowing for data aggregation provides us with new challenges. We need to clarify the meaning of integrity when data aggregation is applied. In aggregation integrity implies that any aggregate result is made up of only legitimate data without inclusions or additions, and that corrupted sensors cannot interfere with operations of the aggregation. We want to be able to assure the base station that the aggregate result it receives is a fair representation of the network state.

In this paper, we propose the use of homomorphic encryption in WSN in order to achieve:

- A solution for confidentiality calculating the SUM and AVERAGE in a wireless sensor network.
- A solution for integrity preserving data aggregation in wireless sensor networks. We are using an additively digital signature algorithm based on ECDSA to achieve integrity of the aggregate result.

II. REVIEW OF LITERATURE

The small size and limited computational power of sensors makes some security protocols such as asymmetric key cryptography difficult to realize. All communication in a WSN uses RF and so it is easy for an attacker to eavesdrop, spoof or inject false messages into the WSN. Due to the amount of time required for the encryption and decryption operations, queues in the network can overflow, leading to dropped packets. Elliptic Curve Cryptography has been implemented for sensors and can be used to distribute necessary keys. Those mechanisms will provide security services like confidentiality, integrity and authenticity, but only for end-to-end security case. They also consume more energy as packet size increases which can restrict service availability of (i.e., ability to securely process) high-rate sensor data streams. Many sensor network applications demand secure communications. Encryption is the preferred way to provide for a secure communication channel. Encryption ensures that only the sender and the intended receiver can read the message contents.

Homomorphic encryption is one technique to solve this problem, as it allows certain aggregation functions such as sum and average to be performed on encrypted data. In this approach, intermediate sensors can perform aggregation without having to decrypt/ encrypt data. The base station receives the encrypted aggregate result and subsequently decrypts it. While homomorphic schemes do provide confidentiality along with aggregation in one step, existing homomorphic encryption and decryption operations are still computationally very energy and time consuming.

Homomorphic encryption is a cryptographic technique which allows calculations to be performed on aggregate data. Specifically, a homomorphic encryption scheme allows the following property to hold:

$$enc(a\oplus b)=enc(a)\oplus enc(b)$$

.

This means that in order to calculate the SUM of two values, we can apply some function to their encrypted counterparts and then decrypt the result of the SUM operation. Clearly, considering the cost of encryption and decryption, homomorphic encryption is useful in wireless sensor networks, because homomorphic encryption would allow for the calculation of SUM and AVERAGE on encrypted data. The data would be encrypted at the sensor node, the SUM or AVERAGE would be calculated as the aggregate result follows a path to the base station, and the final result would be decrypted at the base station. Any eavesdropper would be unable to gather information from the transmissions. Any corrupted sensor could not know the aggregate result.

Elliptic curve cryptography (ECC) employs the points on an elliptic curve over a finite field K. The required algorithms for elliptic curve cryptography can easily be implemented, even on small devices such as sensors. Elliptic curve cryptography uses the analog of the discrete logarithm problem (DLP), also known as the elliptic curve discrete logarithm problem (EC-DLP). The DLP over elliptic curves is believed to be computationally much more difficult than DLP over finite fields of the same size.

Homomorphic encryption does not provide integrity. Since we are using public key elliptic curve cryptography, we will use digital signatures to provide integrity. Digital signature schemes are not homomorphic. That is two signatures generated on two different messages cannot be combined to verify the sum of the messages. We propose the use of an encryption scheme which will allow for homomorphic signature generation and verification.

III. OBJECTIVE

We propose the use of elliptic curve digital signatures to provide message integrity and integrity of the aggregate in addition to data confidentiality. Each node generates a reading. The reading is signed with the aggregate signature protocol using the node's private key; this is shown as Sig(x). Each node homomorphically encrypts the reading with the base station's public key; this is shown as Enc(x) in Figure 1. The node sends the secured reading, the signature and its public key to its parent. After receiving messages from all its children, the parent combines the messages into one. The parent sums the secured readings, the signatures and the public keys. If the parent also contributes a reading, that reading is treated like any other reading. These are shown as SUM−ENC, SUM−SIG and SUM −KEY in Figure 1. This process is repeated by each parent along the path to the base station.

The base station decrypts the received message. The sum of the readings was homomorphically encrypted with the base stations public key. This allows the base station to decrypt the readings. Only the base station which is in possession of the matching private key is able to decrypt the readings. This is shown as Dec(Enc(x)) in the figure. Each node signed its messages, and these signatures were combined along the way. The base station can now verify the sum of the signatures given the sum of the public keys. The aggregate signature protocol ensures that only readings from legitimate sensors are included in the aggregate.

IV. METHODOLOGY

Each sensor is pre-loaded with the appropriate elliptic curve parameters, the base stations' public key and a network wide random integer. The integer is used to generate a new k at set intervals. This ensures that the signatures are additive and secure against attacks. At the start of each round, each sensor chooses a private key and computes the appropriate public key. Choosing a private key is straightforward and requires the sensor to pick an integer in the field of the elliptic curve. The public key is generated by multiplying the base point T with the private key; the result is another point on the curve. A new public/private key pair is necessary during each round of processing because it would only take two signatures for a malicious node to determine another node's private key. Let's say that node A signs a message ma. The signature would be $k^{-1}(ma + za * r(x))$. Any other node would know $^{-1}$ current random integer k. Additionally, each sensor computes the multiplicative inverse of k mod p. Each sensor can now generate its unique signature si. After the signature has been generated, the sensor proceeds to homomorphically encrypt its reading xi. The sensor first maps its reading onto the elliptic curve. After the mapping the reading is encrypted using the EC-IES algorithm. If the sensor receives messages from other nodes for forwarding, it combines them according to the algorithm. The signature scheme is designed such that all signatures can be combined via simple arithmetic. This makes the amount of work required from a parent very small and thus well suited for wireless sensor networks.

We will now describe the base station's algorithm. The base station receives the sum of the signatures, the sum of the algorithm described securely calculates the SUM of the appropriate public keys and the homomorphically encrypted aggregate result. The base station can now verify that the same sensors that contributed to the aggregate also signed their inputs and that signature is included in the combined signature. The base station first decrypts the aggregate result using its private key. Additionally, the base station needs to reverse the mapping from the point on the elliptic curve to the aggregate result. To verify the signature, the base station calculates a point on the curve using the received signature, the decrypted aggregate result and the integer k. If the x-coordinate of the point calculated is the same as r(x), the signature is verified. The base station is now assured that no data not generated by a legitimate sensor was included in the aggregate.

The algorithm described securely calculates the SUM of the readings in a wireless sensor network. In order to securely calculate the AVERAGE in a wireless sensor network, the base station needs a count of the number of points included in the SUM. With the knowledge of how many sensors contributed to the aggregate, the AVERAGE can be calculated

ECDSA has been shown to be secure under the assumption that the underlying group is generic and that a collision resistant hash function has been used. The signature produced by summing the individual signatures will only verify if the contributing individual signatures were produced by a valid node and the appropriate public key was included in the sum of public keys.

We will now prove that the combined signature will only verify if the individual signatures contributed by the nodes are signatures generated by valid nodes and are valid signatures. The value k is a randomized, synchronized integer used by all nodes in the network. We do not need to send r(x) with each signature, as the base station is able to compute r(x). Therefore the unique part of each node's signature is si.

V. CONCLUSION

Secure data aggregation schemes have been of interest to researchers. The earliest approaches focused on confidentiality of the data against a single aggregators. Algorithms which pre vented or detected multiple aggregators colluding to deceive the base station were also introduced. The algorithm guarantees the detection of aggregate modification by the aggregator, except for those cases where the aggregator injects data into the aggregate. The algorithm supports any arbitrary tree structure and is resilient to any number of malicious nodes. The algorithm focuses on the use of the SUM operator, but would also work with MEDIAN, COUNT and AVERAGE. This algorithm forces a commitment from the adversary at intermediate nodes. Each sensor also verifies that its data was properly added to the aggregate. Our algorithm works with any single- path routing protocol, and will securely calculate the SUM and AVERAGE.

The algorithm uses privacy homomorphism to achieve data hiding while still allowing for data aggregation. The algorithm provides for data confidentiality only. The algorithm uses symmetric keys, while our work uses a private/public key approach. The work provides a survey of possible homomorphic public key encryption schemes suitable for wireless sensor networks.

In this paper a novel algorithm is presented to address the problem of secure data aggregation in wireless sensor networks. We apply a homomorphic encryption algorithm to the messages to achieve confidentiality while allowing in-network aggregation. An additively digital signature algorithm based on ECDSA is used to achieve integrity of the aggregate.

I. REFERENCES

1. M.Anand, Z. Ives, and I. Lee, “Quantifying eavesdropping vulnerability in sensor networks,” in *DMSN ’05: Proceedings of the 2nd international workshop on Data management for sensor networks*.New York, NY, USA: ACM Press, 2005, pp. 3–9.
2. P. Levis, N. Lee, M. Welsh, and D. Culler, “Tossim: accurate and scalable simulation of entire tinyos applications,” in SenSys ’03: Proceedings of the 1st international conference on Embedded networked sensor systems. New York, NY, USA: ACM Press, 2003, pp. 126–137.
3. J.Albath and S. Madria, “Practical algorithm for data security (pads) in wireless sensor networks,” in *MobiDE ’07: Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access*. New York, NY, USA: ACM Press, 2007, pp. 9–16.
4. C.Karlof, N. Sastry, and D. Wagner, “Tinysec: A link layer security architecture for wireless sensor networks,” in *Second ACM Conference on Embedded Networked Sensor Systems (SensSys 2004)*, November 2004.
5. L.Clare, G. Pottie, and J. R. Agre, “Self-organizing distributed sensor networks,” *SPIE-The International Society for Optical Engineering*, pp. 229–237, 1999.
6. E.Mykletun, J. Girao, and D. Westhoff, “Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks,” *IEEE International Conference on Communications ICC*, 2006.
7. B.Krishnamachari, D. Estrin, and S. B. Wicker, “The impact of data aggregation in wireless sensor networks,” in *ICDCSW ’02: Proceedings of the 22nd International Conference on Distributed Computing Systems*. Washington, DC, USA: IEEE Computer Society, 2002, pp. 575–578.