Securing and Transmitting Quantum Data on Wireless Sensor Network

G. Subhashini, V. Neelambary

Abstract: ***Signcryption is a cryptographic technique for simultaneously performing both digital signature and data encryption. It is an effective technique for protecting the confidentiality and unforgeability of communications in Internet of Things (IoT) systems, especially when a number of generated cipher texts can be aggregated into a compact form. This paper focus on device capture attacks those are commonly threatening the implementations of signcryption on unattended devices by enabling an attacker to extract the cryptographic key from a captured device. The proposed obfuscator can protect signcryption programs from key-extraction attacks by transforming the programs into unintelligible obfuscated programs. The scheme's security features with respect to obfuscation, confidentiality, and unforgeability have been theoretically proved. Moreover, in comparison with other (non-obfuscatable) aggregate signcryption schemes, the scheme's computational efficiency is positioned at a medium level while the communication cost is also relatively small, with extra unique security features benefiting from obfuscation. Experiments on different devices indicated that the proposed scheme performs reasonably well as expected. The scheme is widely applicable for various scenarios of IoT, where information is sent from unattended leaf nodes to a sink point.***

Keywords: Signcryption; Internet of Things (Iot); Aggregate Signcryption; Sink Point

I. INTRODUCTION

Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. The „thing" in IoT could be a person with a heart monitor or an automobile with built-in-sensors, i.e. objects that have been assigned an IP address and have the ability to collect and transfer data over a network without annual assistance or intervention.

We proposed signcryption method. It has been widely used to protect both the confidentiality and unforgeability of data transmitted via non-trustable open channels. More Number of IoT devices transmit message to the server via intermediate. So the intermediate frequently send the data to the server, it consumes more computational costs and communication overheads. To solve this problem we implements aggregatable signcryption scheme.

Aggregatable signcryption is a cryptographic technique that syntheses aggregate signature and encryption, and allows distinct signcryption ciphertexts that are intended for the same recipient to be merged into a single signcryption ciphertext of a smaller size to enhance efficiency and decrease communication overheads.. The traditional design of security schemes and the standard implementations of cryptographic algorithms are commonly subject to the assumption that the programs are running in well-protected environments. However, for unattended devices deployed at untrustable places, the devices are potentially untrustable computing endpoints, where the implementation and computing process could be completely observed or even controlled. Technically, in such an environment, secret cryptographic keys are potentially vulnerable to attackers. This is a critical security threat to IoT systems, especially for unattended embedded devices (e.g., sensors, tag readers, and road-side units) operating in potentially hostile environments which are exposed to great security threats. Unfortunately, to the best of our knowledge, none of existing aggregatable signcryption schemes can defeat secret-key extractions when a device is captured by an attacker. Once the secret key is exposed to an attacker, the effectiveness of the corresponding security protocol could be completely lost. With the purpose of protecting captured devices from secret-key extraction attacks, we propose an aggregatable signcryption scheme with an obfuscator for the signcryption algorithm, with major contributions and features summarized as follows.

1) This is the first obfuscate able aggregatable signcryption scheme (OASC) in the community.
2) The security properties of the scheme have been proved, and experimental results indicate that the scheme has good performance.

Scope

This paper "Securing and Transmitting Quantum Data on a Wireless Sensor Network" mainly focuses to provide a reliable communication channel, with enhanced confidentiality and unforgeability of communication against device capture attacks in IoT systems with reduced communication overheads and computational costs. It encompasses a specialized signcryption scheme and also has provided security for the network by preventing key force attack that is both obfuscatable and aggregatable at the same time, together with a probably secure obfuscator for the signcryption algorithm. An aggregatable signcryption scheme is used. The devices encrypt the data and generate the signature and send to the server via intermediate.

The intermediate collects all data and sends it to the same destination by aggregating into a compact form. This process involves conversion of n number of cipher text into single secured cipher text. So it avoids communication overheads and computational Costs. Signcryption performs both signature and encryption and guarantee the confidentiality, integrity, and non-repudiation.

Revised Manuscript Received on December 30, 2018.

G. Subhashini, Assistant Professor, Department of Information Technology, St.Joseph's Institute of Technology, Chennai, India.

V. Neelambary, Assistant Professor, Department of Information Technology, St. Joseph's Institute of Technology, Chennai, India.

It overcomes eavesdropping and unauthorized modification attacks.

II. RELATED WORKS

Obfuscatable Aggregatable Signcryption

This work is contributed by Yang Shi[1].The signcryption uses a cryptographic technique for simultaneously performing both digital signature and data encryption. It is an effective technique for protecting the confidentiality and unforgeability of communications in Internet of Things (IoT) systems, especially when a number of generated cipher texts can be aggregated into a compact form. However, device capture attacks are commonly threatening the implementations of signcryption on unattended devices by enabling an attacker to extract the cryptographic key from a captured device. Motivated by this issue, we propose a novel and specialized obfuscatable aggregatable signcryption scheme (OASC) together with an obfuscator for the signcryption algorithm, which has been designed by taking into account that the computational and communication costs should be sufficiently small (light-weighted) to fit applications in resource-constrained embedded devices. The proposed obfuscator can protect signcryption programs from key-extraction attacks by transforming the programs into unintelligible obfuscated programs.

Mitigation Of Channel jamming

The availability of service in many wireless networks depends on the ability for network users to establish and maintain communication channels using control messages from base stations and other users. An adversary with knowledge of the underlying communication protocol can mount an efficient denial of service attack by jamming the communication channels used to exchange control messages. The use of spread spectrum techniques can deter an external adversary from such control channel jamming attacks. We discuss various design trade-offs between robustness to control channel jamming and resource expenditure[3].

Environmental Monitoring

As environmental issues keep gaining increasing attention from the public opinion and policy makers, several experiments demonstrated the feasibility of wireless sensor net- works to be used in a large variety of environmental monitoring applications. Focusing on the assessment of environmental noise pollution in urban areas, we provide qualitative considerations and preliminary experimental results that motivate and encourage the use of wireless sensor net- works in this context[2].

Wireless Network Communication

Wireless sensor network is a group of specialized transducer with communication infrastructure for monitoring and recording at diverse location. There is a need for a secure channel between a sensor node and an internet host, during the integration of wireless sensor networks into the internet of things. By using Security protocols for Sensor networks (SPINS) scheme, it is possible to secure communication. Our scheme has the following advantages, Sensor Network Encryption Protocol (SNEP) that provides confidentiality, two party authentications, integrity, freshness and the micro version of the Timed, Efficient, Streaming, Loss tolerant Authentication Protocol (μTESLA) provides broadcast authentication. Our scheme is very suitable to provide security solution for integrating wireless sensor networks into the internet of things [4].

Trust management In Unattended Wireless Network

Unattended Wireless Sensor Networks (UWSNs) are characterized by long periods of disconnected operation and fixed or irregular intervals between sink visits. The absence of an online trusted third party implies that existing WSN trust management schemes are not applicable to UWSNs. We exploit a set of trust similarity functions to detect trust outliers and to sustain trust pollution attacks. We demonstrate, through extensive analyses and simulations, that the proposed scheme is efficient, robust and scalable [5].

III. SECURING AND TRANSMITTING QUANTUM DATA

In the proposed system an aggregatable signcryption scheme where multiple IoT devices senses the data and send to the server via routing path. The devices encrypt the data and generate a signature and send to the server via intermediate (Aggregator). After spotting the attacker the server will broadcast the attacker. If the devices itself start transferring data using wrong key ,the aggregator system will not establish the communication in case of key mismatching. Thus this scheme proposes the most reliable form of data transmission with less computational costs and communication overheads.

Advantages

- The (2-hop) multipath reinforcement scheme enhances secured channel communication
- The scheme improves security at the cost of network communication overhead.
- Feasibility of wireless sensor network is high.
- This signcryption algorithm can be used in a large variety of environmental monitoring applications.
- Estimation of results is performed through low computation.
- Secure channel is enriched between a sensor node and an internet host.
- Enhanced reserved computational power and limited capacity.
- It possesses perfect resilience against node.
- It captures attacks as well as support for node based revocation and resistance to node replication.

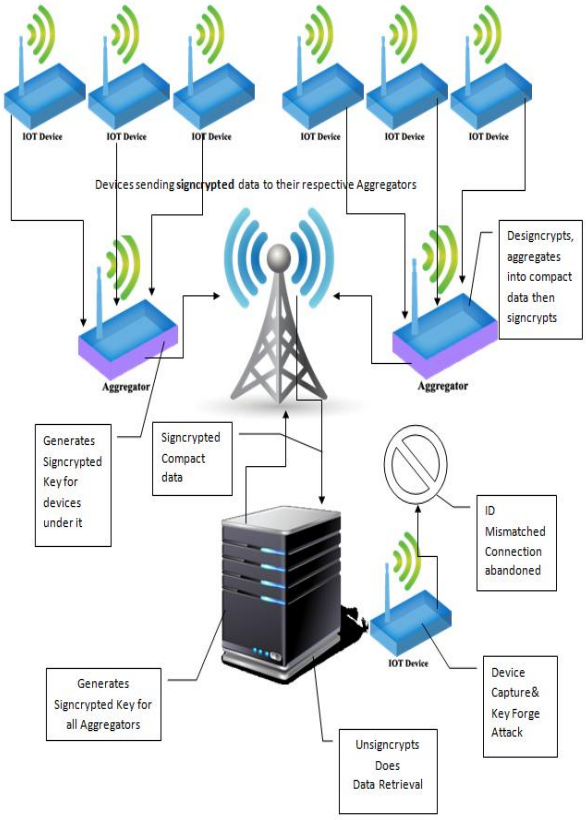

Fig: 1Aggregatablesigncryption in the IoT.

Network Formation

In this module a virtual nodes, devices, aggregators within the certain frequencies and range are being created initially. An Ad-Hoc network is created, which acts as a work station. Aggregator acts an Intermediate between the work station and the devices. Several devices have the regional aggregators through which data is being sent to the adhoc network. Virtual kits are used as devices and the data from the humidity and temperature sensor is collected and send to the aggregator which will be eventually be transmitted to the Work station. The devices are present under the particular aggregator which we consider it as regional aggregator.

We consider a multi-hop Network consisting of a number of virtual kits.

All virtual kits have some ranges. There is a particular range and a distance for each device and based on the distance and range the nearby device is detected and stored in a table for recognising the nearby devices. Two virtual kits ranges are intersect both are neighbours. Each virtual kit finds nearest neighbour and maintains a neighbour list.

A node sends a small amount of information to all other nodes via multi-hop transmission. It is considered as a multi hop network as it transfers data from the device to the aggregator and then to the workstation. The data which is the environmental information such as temperature and humidity readings are transferred to the workstation via the aggregator.

The id of these devices is stored in the aggregator and also the id of the aggregators are also stored in the workstation.

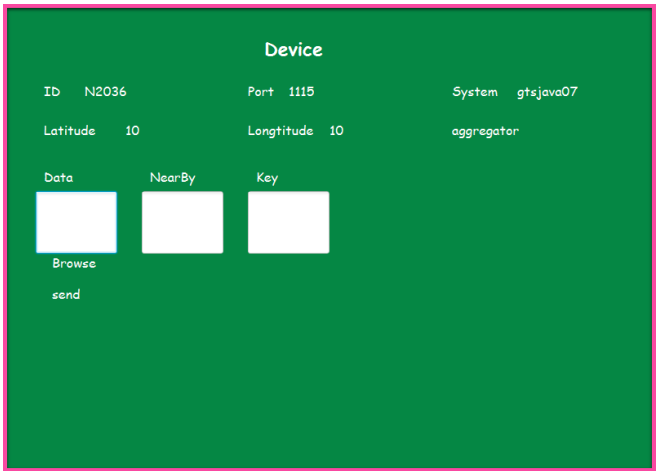

Fig: 2 Node or Network formations

Key Generation & Data Transmission

Each IoT devices sense the information from an environment and transmit to the server via routing path. The device can transmit data only within its range. The device cannot directly communicate with the server, So it uses 326neighbour as an intermediate. More devices choose same intermediate to send the data to the server. The intermediate frequently sends data to the server. Modern cryptographic systems include symmetric-key algorithms (such as DES and AES) and public-key algorithms (such as RSA). Symmetric-key algorithms use a single shared key; keeping data secret requires keeping this key secret. Public-key algorithms use a public key and a private key. The public key is made available to anyone (often by means of a digital certificate). A sender encrypts data with the public key; only the holder of the private key can decrypt this data. The Server provides unique key to each Aggregator. So that the server can recognize the aggregator using the key. Likewise the intermediate or aggregator will provide unique keys to the devices which are under its coverage.

Algorithms Used:-Rivest-Shamir-Adleman (RSA), Hash-Based Message Authentication Code(HMAC).

Fig: 3 Key generations and data transmission

Aggregatable Signcryption & Unsigncryption

Each IoT devices transmit data to its server (workstation) through Aggregator. Every time the IoT device encrypts the data sensed and generates signature for its encrypted data.

Thus unauthorized modification can be overcome using this signcryption technique. In order to include security to the data in the network encryption is done along with digital signature. The data is encrypted using the key that is generated using hmac algorithm and digital signature is also provided and then it is sent to the aggregator and there the data is retrieved by performing Unsigncryption. Using the key of the aggregator again syncryption is performed and the data is transferred to the workstation where the data is unsyncrypted and the original message is retrieved. The secured data will be sent to aggregator, When more than one devices send data to their aggregator it performs data aggregation and generates a compact data which means an aggregated data and start sending to the server (Workstation). The server will perform unsigncrytion and get back the information sent from the aggregator. Once the data received in server it will verify the signatures for the encrypted data. If the signatures are matching there is no modification in encrypted data. If the signature did not match the encrypted data might be modified by someone. When the signatures getting matched, the encrypted contents will be decrypted and the original message will be recovered. This process is called unsigncryption. This is done to increase the security of the data that is sent from the IoT devices. Two specific algorithms are used for Encryption they are Advanced Encryption Standard (AES) and Hash base Message Authentication Code (HMAC).

Algorithms Used

Algorithm 1: Advanced Encryption Standard (AES)

Cipher(bytein[16],byteout[16], key_arrayround_key[Nr+1])
Begin
Byte state[16];
State = in;
AddRoundKey(state, round_key[0]);
for i = 1 to Nr-1 stepsize 1 do
SubBytes(state);
ShiftRows(state);
MixColumns(state);
AddRoundKey(state, round_key[i]);
end for
SubBytes(state);
ShiftRows(state);
AddRoundKey(state, round_key[Nr]);
End

Algorithm 2: hash-based message authentication code(HMAC)

Function hmac (key, message)
if (length(key) >block size) then
// keys longer than block size are shortened
key = hash(key)
end if
if (length(key) <block size) then
// keys shorter than block size are zero-padded
key = key ‖ zeroes(block size - length(key))
end if
// Where blocksize is that of the underlying hash function
o_key_pad = [0x5c * block size] ⊕ key
i_key_pad = [0x36 * block size] ⊕ key // Where ⊕ is exclusive or (XOR)
// Where ‖ is concatenation
Return hash (o_key_pad‖ hash (i_key_pad‖ message))
End function

Fig: 4 Key generations for the data from the device

IV. CONCLUSION

This system enhances the throughput in network delay and uses the resources of workstation server efficiently, This results in reduced communication overheads and computational costs, we have proposed a specialized signcryption scheme that is both obfuscatable and aggregatable at the same time, together with a secure obfuscator for the signcryption algorithm.

V. FUTURE WORK

More the Encryption and signature schemes higher will be the security, Thus to improve the security of signcryption algorithm we can add more encryption and signature generation schemes that will enhance the system with higher security. Here in our system we implemented the signcryption algorithm in stable IOT sensor devices.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

In future enhancement we plan to implement the concept of obfuscatable and aggregatablesigncryption in MANET Environment with devices in mobility.

Ethical clearance: Taken from Research Ethics Committee, Vignan's Foundation for Science, Technology & Research.

Source of funding: Self.

Conflict of Interest: All authors certify that they have participated sufficiently in the work to take public responsibility for the content, including participation in the concept, design, analysis, writing, or revision of the manuscript. Furthermore, each author certifies that this material or similar material has not been and will not be submitted to or published in any other publication.

REFERENCES

1. Yang Shi, Member, IEEE, Jingxuan Han, Xiaoping Wang, JiayaoGao, and Hongfei Fan, Member, IEEE" An Obfuscatable Aggregatable Signcryption Scheme for Unattended Devices in IoT Systems" VOL. 4,AUGUST 2017
2. Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, "A novelapproach to environmental management in unattended wireless sensor networks," IEEE Trans. Mobile Comput., vol. 13, no. 7, pp. 1409–1423, Jul. 2015.
3. P. Tague, M. Y. Li, and R. Poovendran, "Mitigation of control channel jamming under node capture attacks," IEEE Trans. Mobile Comput.,vol. 8, no. 9, pp. 1221–1234, Sep. 2015.
4. L. Shen, J. Ma, X. Liu, F. Wei, and M. Miao, "A secure and efficient ID based aggregate signature scheme orwireless sensor networks," IEEEInternet Things J., to be published, Nov 2014.
5. R. Cheng, B. Zhang, and F. G. Zhang, "Trust management for secure obfuscation of encrypted verifiable encrypted signatures," in Proc. Provable Security, Xi'an,China, 2014, pp. 188–203.
6. X.-Y. Ren, Z.-H. Qi, and Y. Geng, "Provably secure aggregate signcryption scheme," ETRI J., vol. 34, no. 3, pp. 421–428, 2012.
7. D. H. Yum and P. J. Lee, "Exact formulae for resilience in random key pre distribution schemes," IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1638–1642, May 2012.
8. A. Newell, H. Yao, A. Ryker, T. Ho, and C. Nita-Rotaru, "Node-capture resilient key establishment in sensor networks: Design space and new protocols," ACM Comput. Surveys, vol. 47, no. 2, pp. 1–34, 2014.
9. C. Lin, G. Wu, C. Yu, and L. Yao, "Maximizing destructiveness of node capture attack in wireless sensor networks," J. Supercomput., vol. 71, no. 8, pp. 3181–3212, 2015. 55
10. S. Goldwasser and G. N. Rothblum, "On best-possible obfuscation,"J. Cryptol., vol. 27, no. 3, pp. 480–505, 2014.
11. K. Xing and X. Cheng, "From time domain to space domain: Detecting replica attacks in mobile ad hoc networks," in Proc. IEEE Infocom, San Diego, CA, USA, 2010, pp. 1–9.
12. [12] J. M. Bahi, C. Guyeux, M. Hakem, and A. Makhoul, "Epidemiological approach for data survivability in unattended wireless sensor networks," J. Netw.Comput. Appl., vol. 46, pp. 374–383, Nov. 2014.
13. Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, "A novel approach to trust management in unattended wireless sensor networks," IEEE Trans. Mobile Computing., vol. 13, no. 7, pp. 1409–1423, Jul. 2014.
14. B. Barak et al., "On the (Im)possibility of obfuscating programs," J. ACM, vol. 59, no. 2, Apr. 2012, Art. no. 6.
15. B. Barak et al., "On the (Im)possibility of obfuscating programs," in Proc. Adv. Cryptol. (CRYPTO), Santa Barbara, CA, USA, 2001.