Journal of Engineering Sciences

Vol 13, Issue 03, MARCH /2022
ISSN NO:0377-9254

AN EFFICIENT PRIVACY PRESERVING MESSAGE AUTHENTICATION SCHEME FOR INTERNET-OF-THINGS

[1]REVOJU PAVITHRA,[2] MURALI PONAGANTI
[1]MCA Student, [2]Assistant Professor
Department Of MCA
Sree Chaitanya College Of Engineering, Karimnagar

ABSTRACT

As an essential element of the next generation Internet, Internet of Things (IoT) has been undergoing an extensive development in recent years. In addition to the enhancement of people's daily lives, IoT devices also generate/gather a massive amount of data that could be utilized by machine learning and big data analytics for different applications. Due to the machine-to-machine (M2M) communication nature of IoT, data security and privacy are crucial issues that must be addressed to prevent different cyber attacks (e.g., impersonation and data pollution/poisoning attacks). Nevertheless, due to the constrained computation power and the diversity of IoT devices, it is a challenging problem to develop lightweight and versatile IoT security solutions. In this paper, we propose an efficient, secure, and privacy-preserving message authentication scheme for IoT. Our scheme supports IoT devices with different cryptographic configurations and allows offline/online computation, making it more versatile and efficient than the previous solutions.

I. INTRODUCTION:

THE Internet of Things (IoT) provides a self-establishing network of highly coupled heterogeneous objects, such as smart devices, RFID tags, sensors, etc. It allows devices to simplify the retrieval as well as the exchange of data without human involvement in various applications [1] and has a considerable position in the growth of information technology after the computer science and the Internet. IoT brings a pervasive digital appearance by engaging society and industries, and enables a series of interactions between human to human, human to thing, and more importantly, thing to thing. The development of IoT has led to enormous applications, such as smart home systems (SHSs) [2], intelligent transportation systems [3][4], machine learning and big data [5], etc. The machine-to-machine (M2M) [6] communication among massive numbers of IoT devices will dominate future communication network traffic. The integrity and authenticity of the massive amount of data collected and transmitted by the IoT devices are crucial in some applications such as machine learning and big data analytics. Maliciously injected or modified data can cause biased or wrong decision making and prediction. Therefore, in order to ensure the correctness and accuracy of machine learning and big data analysis, the integrity and authenticity of the collected data must be retained [7].

There are two approaches to achieve secure message delivery in IoT: the symmetric-key based approach, and the publickey based approach. The symmetric-key approach incurs less computation overhead compared with the public-key approach since symmetric-key operations are much more efficient than their public-key counterparts. However, key management is a major issue for symmetric-key based approach in a large scale heterogeneous IoT network. Also, if the message is only authenticated using a shared key between the sender and the receiver, the intermediate forwarding nodes in the IoT network cannot verify the integrity of the message. If the message has been altered or damaged during transmission, then the problem can only be discovered by the receiver. On the other hand, public-key based approach can solve these problems since anyone can use the public key to verify the integrity and authenticity of a message. However, public-key operations are very computation intensive, and privacy is another concern for public-key based approach since the authentication token is publicly verifiable using the sender's public key. It is worth noting that the privacy of a data source is also

important in some situations, e.g., when a wearable device is attached to a human. If the attacker can identify the sources of the data streams, then they could also cut off a data stream (e.g., via a Denial-of-Service attack) and eventually affect the accuracy of the decision or prediction produced by machine learning.

In order to address the above problems in IoT and M2M communications, a secure, efficient and privacy-preserving message authentication scheme that can support hop-by-hop verification is desirable. In [8], Li et al. proposed a novel source anonymous message authentication (SAMA) scheme which could be used for such a purpose. Their scheme was believed to achieve message authentication and message source privacy with a lower cost than the previous approaches.

II. EXISTING SYSTEM:

In order to prevent various types of attacks in data transmission, both symmetric-key and public-key approaches have been proposed in the literature. In [12], two different message authentication protocols were proposed. The first protocol, named TESLA, is based on Message Authentication Code (MAC), and the design utilizes a one-way key chain and timed release of keys by the sender. However, the TESLA protocol requires synchronization among devices, which is difficult to implement in a large scale network. The second protocol in [12], named EMSS, is based on cryptographic hash function and public-key technique, and can achieve the security property of non-repudiation.

In [13], an interleaved hop-by-hop authentication scheme was proposed to prevent the injected false data packet attack by attackers or compromised nodes in the network. Their scheme is symmetric-key based, and the basic idea is that multiple sensor nodes have to endorse a message (or report) using MACs in order to achieve message authentication. A similar approach was also proposed in an independent work by Ye et al. [14]. In [15], a polynomial based approach was proposed to achieve lightweight and compromise-resilient message authentication, where messages are authenticated and verified via evaluating polynomials. In [8], Li et al. proposed a ring signature [16] based solution to achieve message authentication. Their scheme utilizes a ring signature scheme derived from the modified ElGamal signature scheme [10], and can achieve better features and performance in several aspects compared with the previous solutions. However, as we will demonstrate later, the ring signature scheme proposed in [8] has a security flaw: it allows an attacker to arbitrarily form a ring and forge a valid ring signature from an existing one. Such an attack has been considered in the literature of ring signature (e.g., [17]) and in this work we introduce a technique similar to that of [17] to fix the flaw without introducing any computation or communication overhead.

There are also a number of research works on privacy preserving user authentication (and key agreement) protocols for IoT and wireless sensor networks (WSNs) in recent years (e.g., [18], [19], [20], [21], [22], [23], [24], [25], [26]). These works focus on remote user authentication, which is related but different from the privacy preserving hop-by-hop message authentication considered in this paper. Moreover, due to the concerns on the physical security of sensor nodes and IoT devices, the research on constructing lightweight and physically secure authentication protocols for IoT and wireless sensor networks has also become a popular topic in recent years. To ensure physical layer security, Physically Unclonable Functions (PUFs) and wireless channel characteristics (such as the Link Quality Indicator (LQI)) are popular choices to enable security even if a sensor node is captured by an adversary. Several novel lightweight authentication protocols with physical security for IoT and WSNs can be found in [27][28][29].

Disadvantages

- The system is less effective due to lack of source location privacy.
- The system has only detection techniques and no protection techniques.

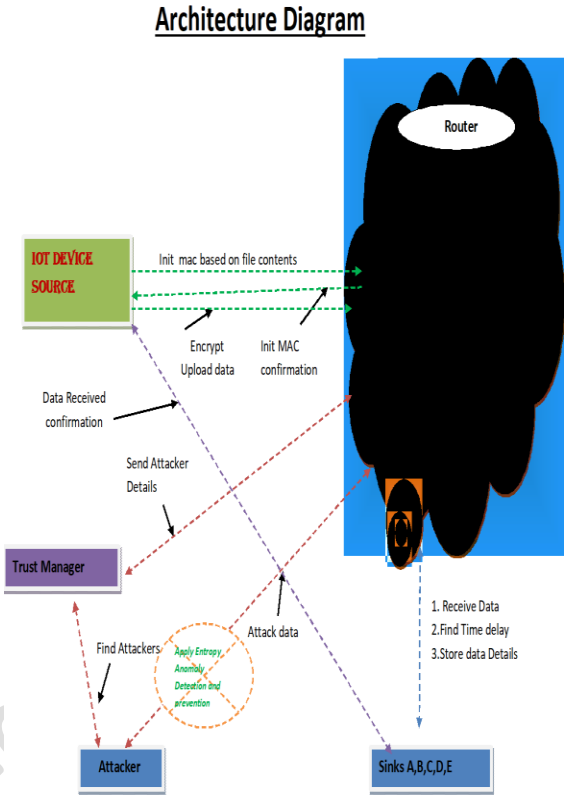
III. PROPOSED SYSTEM:

Moreover, considering the low computation power of the IoT devices, we also apply the offline/online paradigm in the design of our system. Efficiency is extremely important in practical IoT scenarios such as industrial automation, environmental monitoring, smart grids, etc. In proposed scheme, a smart device can perform some expensive public-key operations offline (e.g., when it is idle), and only does the online computation when the message to be sent is ready. Interestingly, we find that by allowing both RSA and ElGamal type systems in our scheme, we are able to reduce the computation cost compared with the pure ElGamal scheme proposed in [8]. This may look counterintuitive since it is known that the ElGamal system (implemented using Elliptic Curve Cryptography, or ECC for short) is much faster than the RSA system. The reason of this counterintuitive fact is that in our hybrid scheme, for most of the RSA nodes, we only need to do RSA signature verification,
which is very fast since the RSA public exponent e can be very small. The proposed new SAMA scheme is compared with the previous scheme in terms of its execution time during signature generation and verification. We also implement our scheme in a laptop and in a Raspberry Pi to demonstrate its practicality.

Advantages

- Authenticity: The receiver and each forwarder in the routing path can verify that the message is sent by a legitimate data source, which can be a specific node, or a node in a particular group.
- Integrity: The receiver and each forwarder in the routing path can verify that the message has not been altered during transmission.
- Identity and location privacy: the identity and location of the message sender is well-protected. As mentioned before, the identity and location of a node may disclose some information about the data sent by that node.

IV. SYSTEM ARCHITECTURE:



V. MODULES:

- **IOT Device Source**

  In this module, the Source browses the required file, initializes nodes with digital signature and uploads to the end user (node a, node b, node c, node d, node e, node f) via Router.

- **Router**

  The Router is responsible for forwarding the data file in shortest distance to the destination; the Router consists of Group of nodes, the each and every node (n1, n2, n3,n4,n5,n6,n7,n8,n8,n10,n11,n12, n13) consist of Bandwidth and Digital Signature(MAC). If router had found any malicious or traffic node in the router then it forwards to the IDS Manager. In Router we can assign the bandwidth for the nodes and can view the node details with their tags Node Name, Sender IP, Injected data, Digital Signature, Bandwidth and status.

- **IDS Manger**
  The IDS manager is nothing but Intrusion Detection System manager which is responsible to filter the malicious data and traffic data. The IDS manager decides the phases based on Router status and then decides on two phases i.e., the "Training Phase" and the "Test Phase".

  Training Phase:
  The Normal Profile Generation module is operated in the Training Phase to generate profiles for various types of legitimate traffic records, and the generated normal profiles are stored in a database.

  Test Phase:
  The Tested Profile Generation module is used in the Test Phase to build profiles for individual observed traffic records. Then, the tested profiles are handed over to the Attack Detection module, which compares the individual tested profiles with the respective stored normal profiles.
- **Sinks**

  In this module, the destination can receive the data file from the Service Provider which is sent via Router, if malicious or traffic node is found in the router then it forwards to the IDS Manager to filter the content and adds to the attacker profile.
- **Forgery Attacker and Packet Droppers**
  In this module, the malicious node or the traffic node details can be identified by a threshold-based classifier is employed in the Attack Detection module to distinguish DoS attacks from legitimate traffic. The Attacker can inject the fake message and generates the signature to a particular node in the router with the help of threshold-based classifier in testing phase and then adds to the attacker profile.

VI. SYSTEM SPECIFICATION:

H/W System Configuration:-

- ➢ Processor - Pentium –IV
- ➢ RAM - 4 GB (min)
- ➢ Hard Disk - 20 GB
- ➢ Key Board - Standard Windows Keyboard
- ➢ Mouse - Two or Three Button Mouse
- ➢ Monitor - SVGA

Software Requirements:

- Operating system : Windows XP or Windows 7, Windows 8.
- Coding Language: Java – AWT,Swings,Networking
- Data Base : My Sql / MS Access.
- Documentation : MS Office
- IDE : Eclipse Galileo
- Development Kit : JDK 1.6

VII. CONCLUSION:

we revisited a privacy-preserving message authentication scheme and showed a security weakness in the scheme. We also provided a solution to fix the problem without introducing any overhead. In order to provide better practicality in IoT consisting of different types of smart devices, we also proposed a new privacy-preserving message authentication scheme that allows IoT devices to use different security systems and parameters. Moreover, we applied the offline/online computation technique to improve the efficiency and scalability of the proposed scheme, which makes it more practical compared with the previous solution.

VIII. REFERENCES:

[1] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey,"
IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–
2243, 2014.
[2] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy

preserving communication protocol for iot applications in smart homes,"
IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1844–1852, 2017.
[3] W. He, G. Yan, and L. Da Xu, "Developing vehicular data cloud services
in the iot environment," IEEE Transactions on Industrial Informatics,
vol. 10, no. 2, pp. 1587–1595, 2014.
[4] J. Wei, X. Wang, N. Li, G. Yang, and Y. Mu, "A privacy-preserving
fog computing framework for vehicular crowdsensing networks," IEEE
Access, vol. 6, pp. 43 776–43 784, 2018.
[5] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, "Deep
learning for iot big data and streaming analytics: A survey," IEEE
Communications Surveys Tutorials, vol. 20, no. 4, pp. 2923–2960, 2018.
[6] J. Shen, T. Zhou, X. Liu, and Y.-C. Chang, "A novel latin-squarebased
secret sharing for m2m communications," IEEE Transactions on
Industrial Informatics, vol. 14, no. 8, pp. 3659–3668, 2018.
[7] P. McDaniel, N. Papernot, and Z. B. Celik, "Machine learning in
adversarial settings," IEEE Security Privacy, vol. 14, no. 3, pp. 68–72,
2016.
[8] J. Li, Y. Li, J. Ren, and J. Wu, "Hop-by-hop message authentication and
source privacy in wireless sensor networks," Parallel and Distributed
Systems, IEEE Transactions on, vol. 25, no. 5, pp. 1223–1232, 2014.
[9] T. ElGamal, "A public key cryptosystem and a signature scheme based
on discrete logarithms," in Advances in Cryptology - CRYPTO '84, 1985,
pp. 10–18.
[10] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in
Advances in Cryptology - EUROCRYPT '96, 1996, pp. 387–398.
[11] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining
digital signatures and public-key cryptosystems," Commun. ACM,
vol. 21, no. 2, pp. 120–126, 1978.
[12] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication
and signing of multicast streams over lossy channels," in Security and
Privacy (S&P), IEEE Symposium on, 2000, pp. 56–73.
[13] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-byhop
authentication scheme for filtering of injected false data in sensor
networks," in Security and Privacy (S&P), IEEE Symposium on, 2004,
pp. 259–271.
[14] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected
false data in sensor networks," Selected Areas in Communications,
IEEE Journal on, vol. 23, no. 4, pp. 839–850, 2005.
[15] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and
compromise-resilient message authentication in sensor networks," in
The 27th IEEE Conference on Computer Communications (INFOCOM),
2008.
[16] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in
Advances in Cryptology - ASIACRYPT 2001, 2001, pp. 552–565.
[17] E. Fujisaki and K. Suzuki, "Traceable ring signature," in International
Workshop on Public Key Cryptography. Springer, 2007, pp. 181–200.
[18] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credentialbased
mutual authentication and key agreement scheme with pseudo
identity for wireless sensor networks," Information Sciences, vol. 321,
pp. 263–277, 2015.
[19] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable
temporal-credential-based two-factor authentication scheme using
ecc for wireless sensor networks," Journal of Network and Computer

Applications, vol. 76, pp. 37–48, 2016.
[20] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, S. Kumari, and
M. Jo, "Chaotic map-based anonymous user authentication scheme with
user biometrics and fuzzy extractor for crowdsourcing internet of things,"
IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2884–2895, 2017.
[21] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari,
"A robust ecc-based provable secure authentication protocol with privacy
preserving for industrial internet of things," IEEE Transactions on
Industrial Informatics, vol. 14, no. 8, pp. 3599–3609, 2017.
[22] M. N. Aman, K. C. Chua, and B. Sikdar, "Secure data provenance for
the internet of things," in Proceedings of the 3rd ACM International
Workshop on IoT Privacy, Trust, and Security. ACM, 2017, pp. 11–14.
[23] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo,
"A three-factor anonymous authentication scheme for wireless sensor
networks in internet of things environments," Journal of Network and
Computer Applications, vol. 103, pp. 194–204, 2018.
[24] D. Wang, W. Li, and P. Wang, "Measuring two-factor authentication
schemes for real-time data access in industrial wireless sensor networks,"
IEEE Transactions on Industrial Informatics, vol. 14, no. 9, pp. 4081–
4092, 2018.
[25] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for
preventing sensitive information inference attacks in social networks,"
IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4,
pp. 577–590, 2018.