A survey on providing security to the wireless sensor networks integrated with IOT

Meghana D K, Monica R Mundada

Abstract— **Integrating the WSN with IoT has many advantages. The data collected from the sensor nodes can be broadcasted to the world by connecting the internet to it. When we integrate Wireless sensor networks(WSN) into internet of things(IOT), providing the security to the data is the main issue. This paper presents a survey of various security issues that arise while integrating the WSNs into the IoT. This paper explains methods of integration front-end proxy solution,gateway solution and TCP/IP solutions and their security issues. And also gives some security strategies that can be used when providing security to WSN connected to Internet. Thisprovide security solution for integrating a WSN into the IoT.**

Index Terms— **Front-end proxy solutions,Gateway solution, Internet of things, TCP/IP Solution,Wireless sensor network.**

I. INTRODUCTION

THE Internet of Things (IoT) is a novel paradigm thathas received considerable attention in recent years from both academiaand industry. The basic idea of IoT is the pervasive presencearound us of a variety of things which, through unique addressingschemes, are able to interact with each other and cooperatewith their neighbors to reach common goals [1]-[5]. The Internet of Things connects things from various aspects of the physical world. IoT finds its application in Smart Homes, Smart City, Transportation, Agriculture, Emergency, Health Care and Environment.

Wirelesssensor networks (WSNs) are ad hoc networks which usually consist of a large number of sensor nodes with limited resources and base stations. Usually, sensor nodes consist of a processing unit with limited computational power and limited capacity. On the other hand, the base station is a powerful trusted device that acts as an interface between the network user and the nodes. WSNs have many applications, including military sensing and tracking, environment monitoring, target tracking, healthcare monitoring, and so on. A user of the WSNs can read the data received from the sensors through the base station. Wireless sensor networks have gained so much attention over the last few years .They allow us to gather information about the surrounding environment and sense data from previously inaccessible areas. Advantage of sensor networks is versatility- many configuration modes and various types of sensors that make them suitable for a wide range of applications.

Manuscript received December 22, 2014.

Meghana D K, Mtech Student, Dept of CSE, MSRIT, India.

Monica R Mundada, Associate Professor, Dept of CSE, MSRIT, India.

It is a great challenge to implement security in wireless sensor networks because of the nature of wireless communications, resource limitation on sensor nodes, size and density of the networks, unknown topology prior to deployment, and high risk of physical attacks to unattended sensors [6][7].

II. INTEGRATING WSN WITH IOT

There are three methods to accomplish this integration[8], front-end proxy solution, gateway solution and TCP/IP overlay solution [9].

In a front-end proxy solution, the base station serves as an interface between sensor network and the Internet. The base station collects and stores all the information coming from the sensor network, and also sends any control information to the sensor nodes. There is no direct connection between the Internet and a sensor node. All incoming and outgoing information will be parsed by the base station. As the sensor network is completely independent from the Internet, it can implement its own protocols and algorithm.

In the gateway solution, the base station acts as an application layer gateway, in charge of translating the lower layer protocols from both networks. As a result, the sensor nodes and the Internet hosts can exchange information directly. In this approach, the sensor network can still maintain some of its infrastructural independence, although it is necessary to create a translation table that maps the sensor node addresses to IP addresses.

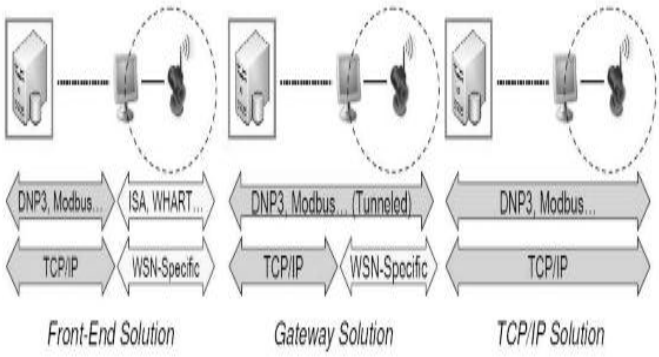

Fig 1. Integration of sensor nodes into Iot

In the TCP/IP overlay solution, sensor nodes do communicate with other nodes using TCP/IP. Therefore, the main function of the base station is to behave as a router, forwarding the packets from and to the sensor nodes. These nodes must implement the protocols and standards used on the Internet, such as the TCP/IP stack and web services interfaces.

Currently, there exist implementations and specifications for IPv4 and IPV6 in sensor nodes.

III. SECURING THE INTEGRATION STRATEGIES

The security for the integration strategies is analyzedas[10].

A. *Front-end proxy solution.*

In a front-end proxy solution, the base station acts as a representative of all the sensor nodes. It provides all the functionality of the network, behaving as an Internet host. Therefore, most protection mechanisms can be implemented and deployed in the base station. As the Internet and the sensor network are logically separated, it can be possible to protect the information exchange between an Internet host and the base station by using any of the existing security standards, while any interaction between the base station and the sensor nodes can make use of simpler security approaches.

Note that, in this case, the base station becomes a single point of failure: if the base station is successfully attacked, an adversary may have access to all the information flow. Moreover, if the base station malfunctions, the sensor network will be completely inaccessible. A possible solution is to use multiple base stations with the purpose of improving the availability of the network in case of base station failure and including new features such as load balancing.. In this front-end proxy solution, the base station and the sensor nodes can make use of simpler mechanisms such as pre-negotiated shared keys, or even public key cryptography. Regarding authentication, as all nodes are considered to be under control of the base station, such base station can authenticate itself (e.g. present its own digital certificate) on behalf of its sensor nodes. User authentication is also managed by the base station, either by using public key certificates or other authentication mechanisms such as (user, password) pairs.

About authorization, the base station can either analyze the credentials presented by the users (e.g. attribute certificates) or check whether the user is authorized to perform certain operations (e.g. by using access control lists – ACL). About accountability, there can be a close collaboration between the sensor nodes and the base station to control and monitor the actual state of the network. The base station can store any interaction between the hosts and the motes, and can also retrieve and analyze any behavioral-related information from the nodes themselves. Also, it can monitor whether a certain node is accessible or not, forwarding any control information if the node becomes available again.

B. *TCP/IP overlay solution.*

By considering the Internet and the sensor network as separate entities, it is not necessary to use the already limited resources of the sensor nodes to implement costly Internet standards. However, this situation changes in the TCP/IP overlay solution, where the sensor nodes become Internet hosts. As a result, the sensor network should be no longer treated as an independent entity, and both the protocols and the security mechanisms that are used in the Internet hosts should also be supported by the sensor nodes. However, for network layer security, IPsec is currently not supported, and it is not clear whether sensor nodes will be able to support the use of these low-level security mechanisms that have end-to end properties. 6lowpan advises to identify the relevant security model and a preferred set of cipher suites that are appropriate given the constraints .Even if there is no support for an end-to-end secure channel at the network layer, most applications still may needto create such channel to protect the information flow. This issue can be partially solved by providing security at the transport layer, using the TLS/SSL standard. In order to save enough resources.

In addition, there is no certificate parsing code, thus clients may need to authenticate themselves using other mechanisms such as passwords. Precisely, regarding user authentication, it may not be feasible to store user credentials (i.e. user and password pairs) inside a sensor node. In this case, all the sensor nodes that belong to the same network should create a mechanism for storing and maintaining such credentials. The same problem applies to user authorization: it would be necessary to maintain the access control model in a distributed form, which is an extremely difficult task.

For authentication, the sensor nodes just need to check the ticket provided by the ticket granting server. Kerberos can also pass authorization information generated by other services. Of course, Kerberos requires continuous availability of a central server, and all devices must maintain their clocks loosely synchronized. Note that PKC solutions (identity certificates, attribute certificates) can also be applied if supported. The low storage capacity of highly constrained nodes significantly hinders the accountability of the network. Sensor nodes should be intelligent enough to detect an abnormal situation caused by hosts accessing to its services, and only store information related to these incidents. In addition, storage capacity partially influences availability: a single node can only store its readings for a limited time, thus the historic data should be either stored elsewhere of summarized somehow.

C. *Gateway solution.*

Some of the challenges that are associated with the TCP/IP overlay solution can be partially solved using the gateway solution. The gateway (i.e. the base station) can take the role of storing the accountability information regarding the interactions between hosts and motes. It also can store the historic data of the nodes, if they have the risk of running out of storage space. In addition, it can improve the availability of the network acting as a “cache server” or as an intelligent forwarder, like in the front-end proxy solution. On the other hand, if end-to-end secure channels are negotiated, it should be necessary to implement non-trivial mechanisms in the gateway to parse the information between an Internet host and a sensor node.

The important requirements for a secure communication are confidentiality, integrity, authentication and nonrepudiation. Confidentiality is keeping the information secret from all other than those who are authorized to see it. Integrity is ensuring that the information has not been altered by unauthorized entities. Authentication is the assurance that the communicating party is the one that it claims to be. Nonrepudiation is preventing the denial of previous commitments or actions. Usually, we use encryption schemes

to achieve the confidentiality and digital signature schemes to achieve the integrity, authentication and nonrepudiation.

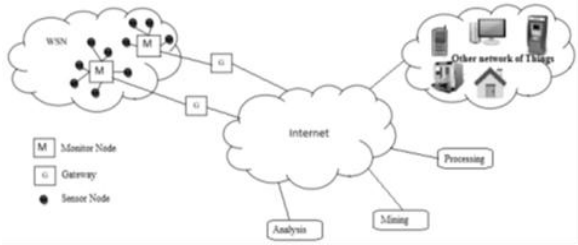

Fig 2. Integrated Solution

There are three main requirements to design the short signature schemes[11][12]. Due to the rigorous pressure of the bandwidth, short signatures are most favorable with respect to the efficiency. Secondly, existential unforgeability, which ensure the adversary cannot even produce a new signature for any previously signed message, are very desirable too. Thirdly, in the multi-user setting, we considerate the non-repudiation is very important. The biggest difference between existential unforgeability and non-repudiation is that the non-repudiation does not generate a brand-new signature by means of the previously signed message. If we need to achieve simultaneously confidentiality, integrity, authentication and nonrepudiation, a traditional approach is first to sign a message and then to encrypt it, called the sign-then encrypt or signature-then-encryption approach.

The main security goals include data privacy, integrity, availability, information and entity authentication. The first goal can be fulfilled by incorporating a link layer security mechanism. Guaranteeing availability involves minimizing the impact of DoS attacks. Authentication ensures the receiver that the message did originate from the claimed sender. In many cases the confidentiality of simple sensor readings is not as important as the origin of the data.

All of the above security requirements can be fully addressed only by building upon a solid key distribution framework. Key management is an essential cryptographic mechanism upon which other security primitives are built.

The cryptography strategies[13][14] that we can use for the securing the data are

A. Public key infrastructure

In the PKI system, a certificate is issued by certificate authority(CA) which provides a unforgeable and trusted link between the public key and the identity of the user by the signature of the user. The disadvantage of the PKI is that we need to manage the certificates. And also before using the certificates we should verify the validity of certificates.

B. Identity based cryptosystem

In the IBC system[15]-[17], from the identity information of the user, user's public key can be derived. Ex: from telephone number, email address etc. Secret keys are generated by the trusted third party called private key generator (PKG) for users. The PKG uses master key to decrypt any message The system ensures that only legitimate recipient can decode such a message. So the keys are self-authenticated. Authenticity of a public key is explicitly verified without any certificates.

Advantage of IBC is that we eliminate the need for certificates. And also that we do not have to store so many public keys. We generate a public key for a given node only when we want to communicate with that node for the first time. IBE allows us to send secure messages without any prior interaction with the given sensor node.

The dependence on the PKG who generate all users' secret keys inevitably causes the key escrow problem [18].

C. Signcryption

Signcryption [19]-[25] is a new cryptographic primitive that fulfills both the functions of digital signature and public key encryption in a logical single step, at a cost significantly lower than that required by the traditional signature-then-encryption approach. That is, signcryption can simultaneously achieves confidentiality, integrity, authentication and non-repudiation at a lower cost. The performance advantage of signcryption over the signature-then-encryption method makes signcryption useful in many applications, such as electronic commerce, mobile communications and smart cards.

D. Combining IBE and PKI

Setup a secure channel between a sensor node and an internet host that supports end-to-end confidentiality, integrity, authentication and non-repudiation services. We require that the IBC is used in the sensor node and that the PKI is used in the internet host.

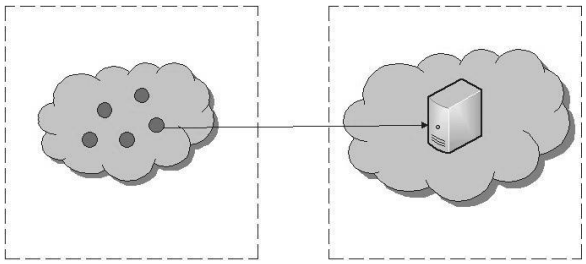

Fig 3.Communication model for integrating WSNs into the Internet.

IV. CONCLUSION

Combining the Wireless sensor networks and Internet of Things has many advantages. But while connecting the internet to the sensor nodes providing security is main issue. Using proper key management scheme like PKI, IBE or combining both can provide a secure communication between the sensor nodes and internet hosts.

ACKNOWLEDGMENT

This work is supported by the management of MSRIT, K.G.Srinivas, HOD, Computer Science and Engineering department and Dr. Monica R Mundada, Associate Professor. Dept of CSE, MSRIT, Bangalore. And I also like to thank the authors of the paper which I have referenced.

REFERENCES

[1]. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2]. Lu Tan, Neng Wang, "Future Internet: The Internet of Things", 3rd International Conference on Advanced Computer Theory and Engineering, pp. 376-380, 2010.

[3]. Luigi Atzori, Antonio Iera ,GiacomoMorabito," The Internet of Things: A survey", Computer Networks, pp.2787-2805,2010.

[4]. Daniel Corujo, Marcelo Lebre, Diogo Gomes, Rui L. Aguiar, "A Framework for the Connectivity of an Internet of Things", Sensors, 2011 IEEE, pp. 643 – 646, 2011.

[5]. SyeLoongKeoh, Sandeep S. Kumar, and HannesTschofenig," Securing the Internet of Things:A Standardization Perspective", ieee internet of things journal, vol. 1, no. 3,pp. , 265-275 , June 2014.

[6]. ZoranBojkovic, BojanBakmaz, MiodragBakmaz , "Some Security Trends over Wireless Sensor Networks", 12th WSEAS International Conference on COMMUNICATIONS, Heraklion, Greece. pp. 470-474. 2008.

[7]. Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz," Security Issues in Wireless Sensor Networks", International Journal Of Communications,Issue 1, Vol 2, pp. 106-115, 2008.

[8]. Fagen Li and Pan Xiong, "Practical Secure Communication for Integrating Wireless Sensor Networks Into the Internet of Things" Sensors Journal, IEEE Vol13 , Issue: 10 pp : 3677 – 3684, : 2013.

[9]. M.Tharani, N.Senthilkumar, "Integrating Wireless Sensor Networks into Internet Of Things For Security", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Issue 1,pp. 467-473,March 2014.

[10]. R. Roman and J. Lopez, "Integrating wireless sensor networks and the Internet: A security analysis," *Internet Res.*, vol. 19, no. 2, pp. 246– 259, 2009.

[11]. Dan Boneh, Xavier Bohen, "Short Signatures Without Random Oracles", Advances in Cryptology—EUROCRYPT 2004, volume 3027 of Lecture Notes in Computer Science, pp. 56–73, 2004.

[12]. Huo Shao, XinglanZhang,Feng Shao, "Cryptanalysis of short signature scheme without random oracles assumptions."International Conference on Computational Intelligence and Security, Vol 1,pp. 414 – 417, 2009.

[13]. S. A. Camtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," Department of Computer Science, Rensselaer Polytechnic Institute, Tech. Rep. TR-05-07, March 23 2005.

[14]. M.A.Simplcio Jr., P.S.L.M.B., C.B Margia, T.C.M.B. Carvalho, *A survey on key management mechanisms for distributed Wireless Sensor Networks.* Computer Networks, 2010. **54**(15).

[15]. S. Cui, P. Duan, C.W. Chan, and X. Cheng,"An efficient identity-based signatures scheme and its applications," *Int. J. Netw. Security*, vol. 5,no. 1, pp. 89–98, Jul.2007.

[16]. PiotrSzczechowiak and Martin Collier, "TinyIBE: Identity-Based Encryption for Heterogeneous Sensor Networks".

[17]. L. Chen and J. Malone-Lee, "Improved identity-based signcryption,"in Public Key Cryptography(Lecture Notes in Computer Science),vol. 3386. New York, NY, USA: Springer-Verlag, 2005, pp. 362–379.

[18]. Mark P Hoyle and Chris J Michell "On solutions to the key escrow problem*".*

[19]. F. Bao and R. H. Deng, "A signcryption scheme with signature directly verifiable by public key," in Public Key Cryptography(Lecture Notes in Computer Science), vol. 1431. New York, NY, USA: Springer-Verlag, 1998, pp. 55–59.

[20]. Fagen Li, Hui Zhang, Tsuyoshi Takagi, "Efficient Signcryption for Heterogeneous System" IEEE system Journals, vol 3, no. 3 Pp 420- 429, 2013.

[21]. F. Bao and R. H. Deng, "A signcryption scheme with signature directly verifiable by public key," in *Proc. PKC*, LNCS 1431.1998, pp. 55–59.

[22]. B. Libert and J. J. Quisquater, "A new identity based signcryptionschemes from pairings," in *Proc. IEEE Inform. Theory Workshop*, Mar.–Apr. 2003, pp. 155–158.

[23]. Hassan M. Elkamchouchi, YasmineAbouelseoud, Eman F. Abu Elk hair, "An Efficient ID Based Proxy Signcryption Scheme without Bilinear Pairings", International Journal of Computer Applications, Vol 76, No.16 pp 11-16.August 2013.

[24]. Benoit Libert, Jean-Jacques Quisquater, "New identity based signcryption schemes from pairings".

[25]. Fagen Li, Tsuyoshi Takagi, "Secure identity-based signcryption in the standard model".