ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Secure Data Transmission with BLAKE2 Algorithm in E-Health care System

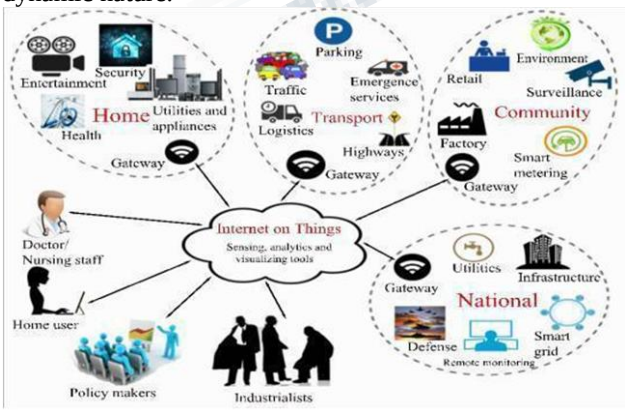
[1] K.Ilakkya, [2] K.Ramya
[1] Final Year PG CSE Student, [2] Asst. Prof of CSE
[1][2] Sree Sowdambika College of Engineering, Aruppukottai, Tamilnadu, India

***Abstract* – The body sensor sort out (BSN) development is a champion among the most fundamental headways used as a piece of IoT-based present day human administrations system. In this Procedure, at first we address the few security requirements in BSN based present day human administrations system. By then, we propose a safe IoT based social protection structure using BSN, called BSN-Care, which can guarantee to successfully complete those requirements.BSN configuration made out of wearable and implantable sensors. Each sensor center is composed with bio-sensors, for instance, Electrocardiogram (ECG)Electromyography (EMG), Electroencephalography (EEG), Circulatory strain (BP), et cetera. These sensors accumulate the physiological parameters and forward them to a facilitator called Nearby Handling Unit (LPU).The LPU goes about as a switch between the BSN center points and the central server called BSN-Care server, using the remote correspondence mediums, for instance, compact frameworks 3G/CDMA/GPRS. In addition, when the LPU perceives any varieties from the standard then it gives provoke alert to the person that wearing the bio-sensors. In this wander, we delineate the key security necessities in IoT based social protection system using BSN.**

Index Terms— Internet of things (IoT), authentication, key establishment, Burrows-Abadi-Needham (BAN) logic, AVISPA, NS2 simulation, security.

INTRODUCTION

IoT encompasses a system of physical objects that are interconnected to exchange and collect data over the internet. These objects are equipped with the required processing and communication abilities and possess a locatable Internet Protocol address (IP address). The objective here is to integrate computer-based systems and the physical world for economic benefit and to improve accuracy and efficiency while reducing human involvement. Cyber-physical systems such as smart grids and intelligent transportation can enormous threat to security and privacy due to its heterogeneous and dynamic nature.



Authentication model for IoT applications.

1) IoT AUTHENTICATION MODEL

In the given IoT authentication model shown in Fig. 1 , we consider four different scenarios, i.e., Home, Transport, Community and National. All these scenarios have smart devices, such as sensors and actuators. These devices facilitate the day to day life of people. In the given scenarios, all smart devices are connected to the Internet through the gateway nodes (GWNs). Different types of users (for example, smart home user and doctor) can access the data of relevant IoT devices through the GWN. Mutual authentication between a user and a device through the GWN provides access to device data to the user.

2) THREAT MODEL

We follow the widely-accepted Dolev-Yao threat (DY) model. Under the DY model, communication between two entities is performed over a public channel. An adversary can then have an opportunity to eavesdrop, modify or delete the content of the messages being transmitted. It is further assumed that the adversary can physically capture one or more sensing devices in IoT, and can extract all the sensitive information stored in the captured devices using the power analysis attacks [4], [5].

B. OUR CONTRIBUTION

The contributions of this paper are:

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

- An authentication model for IoT is presented and the security challenges involved and its requirements are discussed.
- A secure signature-based authentication and key agreement scheme has been proposed to address these issues. - A formal security analysis using BAN logic and an informal security analysis have been presented to prove that the scheme is secure.
- Simulation using the AVISPA tool for the formal verification of the scheme's security has also been provided.
- Using NS2 simulator, the scheme's impact on network performance parameters has been measured for practical demonstration of the scheme.
- Finally, it has been shown that the scheme is also efficient in terms of communication and computation costs.

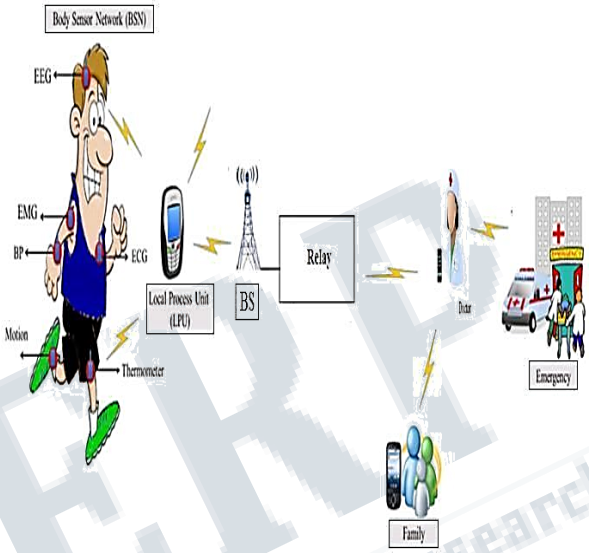
BLAKE2 Security Algorithm:

- BLAKE2 is a cryptographic hash function faster than MD5, SHA-1, SHA-2, and SHA-3, yet is at least as secure as the latest standard SHA-3. BLAKE2 has been adopted by many projects due to its high speed, security, and simplicity.
- BLAKE2 is specified in RFC 7693, and our code and test vectors are available on GitHub, licensed under CC0 (public domain-like). BLAKE2 is also described in the 2015 book The Hash Function BLAKE.
- BLAKE2s is optimized for 8- to 32-bit platforms and produces digests of any size between 1 and 32 bytes.
- BLAKE2 includes the 4-way parallel BLAKE2bp and 8-wayparallel BLAKE2sp designed for increased performance on multicore or SIMD CPUs. BLAKE2 offers these algorithms tuned to your specific requirements, such as keyed hashing (that is, MAC or PRF), hashing with a salt, updatable or incremental tree-hashing, or any combination thereof. These versions are specified in the BLAKE2 document.
- BLAKE2 also includes the BLAKE2x variants, which can produce digests of arbitrary length. BLAKE2x is specified in a separate document.
- BLAKE2 shines on 64-bit CPUs: on an Intel Core i5-6600 (Skylake microarchitecture, 3310MHz), BLAKE2b can process 1 gibibyte per second, or aspeed rate of 3.08 cycles per byte.The plot below shows how BLAKE2 outperforms MD5, SHA-1, SHA-2, and SHA-3 on a Skylake Intel CPU (speeds are for hashing using a single core; using multiple cores, BLAKE2 can be even faster):

II. MATHEMATICAL PRELIMINARIES

In this section, we briefly discuss the properties of an elliptic curve over a finite field.

$$y^2 \equiv x^3 + ax + b \pmod{p},$$



number of points on curve Ep(a,b) , denoted as #E, satisfies the following inequality [6]:

$$p + 1 - 2\sqrt{p} \le \#E \le p + 1 + 2\sqrt{p}$$

In other words, there are about p points on an elliptic curve Ep(a,b). In addition, Ep(a,b) forms a commutative or an abelian group under addition modulo p operation with O as the additive identity and $-P \in Ep(a,b)$ as the additive inverse of the point $P \in Ep(a,b)$.

A. ELLIPTIC CURVE POINT ADDITION

Suppose G is the base point on Ep(a,b) with order n, that is, nG = G+G+...+G(n times) =O. Let P,Q Ep(a,b) be two points on the elliptic curve. Then, R = (xR,yR) = P + Q is calculated as follows [6]:

$$xR = (\lambda^2 - xP - xQ) \pmod{p}, \quad yR = (\lambda(xP - xR) - yP) \pmod{p},$$

$$\lambda = \frac{yQ - yP}{xQ - xP} \pmod{p}, \text{ if } P \neq Q \text{ where } \lambda = \frac{3x^2 + a}{2yP} \pmod{p}, \text{ if } P = Q.$$

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

B. ELLIPTIC CURVE POINT SCALAR MULTIPLICATION

The elliptic curve multiplication is done as repeated additions. For example, 5P = P + P + P + P + P where

III. SECURITY CHALLENGES AND REQUIREMENTS IN IoT APPLICATIONS

As accessibility and global connectivity are the key requirements of any IoT application, it increases the available avenues of threats and attacks. The heterogeneous nature of IoT further raises complexity in the deployment of security mechanisms. The wireless nature of most involved
entities and their limited capacity are also problematic. Possible transient and random failures are vulnerabilities that attackers could exploit. The various possible attacks on IoT applications are as follows:

• ***Denial-of-Service:*** Apart from conventional denial-ofservice (DoS) attacks like exhausting resources and bandwidth, IoT can be susceptible to attacks on communication infrastructure like channel jamming. Adversaries who are privileged insiders can gain control of the relevant infrastructure to cause more chaos in the network.

• ***Controlling:*** Active attackers can gain partial or full control of IoT entities and the extent of damage that can be caused is based on the following:
− Services being provided by the entity.
− Relevance of the data being managed by that entity.

• ***Eavesdropping:*** This is a passive attack through which information can be gathered from channel communication. A malicious insider attacker can also gain more advantage by capturing infrastructure or entities.

• ***Physical damage:*** The easy accessibility of IoT entities and applications can be exploited by attackers to cause physical harm hindering services by attacking an entity or the hardware of the module creating it virtually. Attackers lacking technical knowledge and wanting to cause considerable damage can utilize this.

• ***Node capture:*** Easy accessibility can also be a vulnerability for information extraction through capturing entities and trying to extract stored data. This is a major threat against data processing and storage entities.

The countermeasures to recover from such attacks once they are detected and diagnosed should be lightweight due to the limited capacity of the involved entities. The solutions must be real-time in nature and if possible, a part of self-healing infrastructure. The following are some requirements for IoT to counter security breaches:

• ***Reliability:*** The aim is to guarantee information availability while efficiently managing data storage. Providing redundancy among communication channels through multiple paths is one way to ensure availability.

• ***Responsibility:*** Otherwise known as access control, this ensures legitimate access to services by defining privacy constraints. The rules for each entity and possible liabilities must be clearly defined to avoid damages.

• ***Privacy:*** Owing to the ubiquitous nature of IoT, providing privacy is very important. There are the following three areas where privacy has to be ensured:

− ***Data sharing and management***: This can be achieved by enumerating data aggregated at the sensors. Also, privacy-preservation techniques can be used. − Data collection: Some cryptographic approaches mentioned in and can be used. − Data security: This can be ensured through password protection.

• ***Trust:*** IoT being dynamic and distributed, ensuring trust among interacting entities is important. In a heterogeneous network like IoT where devices and not just humans can be involved in trust management, resource constraints should also be considered while developing techniques.

• ***Safety:*** System components can be prone to sudden failures and safety is required to reduce damage possibilities.

• ***Identification and authentication:*** Privacy and secure access can be ensured primarily through this. As global access is a necessity in IoT, entities could have one permanent and several temporary identities. IV.

IV. PROPOSED SCHEME

In this section, we present a new signature-based authenticated key establishment scheme using the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

authentication model for IoT applications provided in Fig. 1. As shown in this figure, different users communicate with each other and with various smart devices through gateways to ensure secure communication. The proposed scheme can be applied in all kinds of the IoT applications. For example, a doctor can remotely monitor a patient's vitals through the readings recorded by sensing devices in wireless body area networks. A home user can detect any intrusion by monitoring smart meter readings. In the proposed scheme, a legal user can access the information from a sensing device in the IoT applications provided that both mutually authenticate each other. After their mutual authentication, a secret session key will be established between them for their future secure communications.The notations used in detailing the proposed scheme have been listed in Table 1. To protect the proposed scheme from strong replay attack, we use both random numbers as well as

TABLE 1. Notations used in this paper.

Symbol	Description
GWN	Gateway node
SD_j	j^{th} sensing device
ID_j	SD_j's identity
U_i	i^{th} user
SC_i	U_i's smart card
ID_i	U_i's identity
PW_i	U_i's password
BIO_i	U_i's personal biometrics template
σ_i	Biometric secret key
τ_i	Biometric public reproduction parameter
t	Error tolerance threshold used by fuzzy extractor
$Gen(\cdot)$	Probabilistic generation procedure used by fuzzy extractor
$Rep(\cdot)$	Deterministic reproduction procedure used by fuzzy extractor
$h(\cdot)$	Collision-resistant one-way cryptographic hash function
p	A large prime number
Z_p	$Z_p = \{0, 1, \cdots, p-1\}$, a prime finite field
E_p	An elliptic curve over prime field Z_p
$P = ((P)_x, (P)_y)$	an elliptic curve point in elliptic curve E_p, $(P)_x$ and $(P)_y$ are x and y coordinates of P, respectively
$k.P$	Elliptic curve point multiplication; $k \in Z_p^*$ being a scalar and $P \in E_p$
d	private key of involved entities
Q	$Q = d.P$, public key of involved entities
T_i, T_s	Current system timestamps
ΔT	Maximum transmission delay
sk_{ij}	Session key between U_i and SD_j
$\oplus$, $\|\|$	Bitwise XOR and concatenation operations, respectively

current timestamps. For this reason, we assume that all the entities involved in IoT environment are synchronized with their clocks. The proposed scheme consists of the following eight phases, namely, 1) system setup, 2) sensing device registration, 3) user registration, 4) login, 5) authentication and key agreement, 6) password & biometric update, 7) smart card revocation and 8) dynamic sensing device addition. The detailed descriptions of these phases are discussed in the following subsections.

V. SECURITY ANALYSIS OF THE PROPOSED SCHEME

In this section, we first prove that the proposed scheme provides secure mutual authentication between a user Ui and a sensing device SDj with the help of the widely-accepted BAN logic. Furthermore, we show that the proposed scheme is secure against various known attacks informally. In addition, the formal security verification using the broadly-accepted AVISPA tool ensures that the scheme is also secure against replay and man-in-the-middle attacks.

A. MUTUAL AUTHENTICATION USING BAN LOGIC

To prove that a user Ui and a sensing device SDj mutually authenticate each other through fresh and trustworthy information, the BAN logic is being used. This is achieved by verifying the message's origin, the origin's freshness and trustworthiness. The following notations are used in the BAN logic:

• A |≡ X: A believes the statement X.

• A G X: A sees X, i.e. A has received a message containing X.

• #(X): X is a fresh message. K

• A ←→ B: K is shared secret key between A and B.

• XK : X is encrypted with key K.

• < X >Y : formula X is combined with formula Y.

• (X)K : X is hashed with key K.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

• (X,Y): X or Y is one part of formula (X,Y). The logical postulates in the BAN logic are described using the below mentioned rules:

Rule 1 (Message Meaning Rule (MMR)): P believes Q once said X if P sees a message X encrypted with K and P believes K is a shared secret between P and Q.

$$\frac{P \models P \overset{K}{\longleftrightarrow} Q, P \triangleleft \{X\}K, \quad P \models Q \mid\sim X}{P \models P \overset{Y}{\longleftrightarrow} Q, P \text{ Ch} X \text{i} Y}$$

Rule 2 (Nonce Verification Rule (NVR)): P believes Q believes X if P believes Q once said X and P believes X is fresh. P

Rule 3 (Jurisdiction Rule (JR)): P believes X if P believes that Q believes X and P believes Q has jurisdiction over X.

$$\frac{P \models Q \models X, P \models Q \text{ p}\Rightarrow X}{P \models Q \models X}$$
$$P \models X$$

Rule 4 (Freshness Rule (FR)): The entire formula is believed to be fresh if a part of the formula is believed to be fresh, .

$$\frac{P \models \#\{X\}}{P \models \#\{X,Y\}}$$

Rule 5 (Belief Rule (BR)): P believes Q believes part of the formula if P believes Q believes a formula,

$$\frac{P \models Q \models (X,Y)}{P \models Q \models X}$$

P believes combined formula (X,Y) if P believes X and P also believes Y.

$$\frac{P \models X, P \models Y}{P \models (X,Y)}$$

G1: $Ui \models Ui \overset{skij}{\longleftrightarrow} SDj$,

G2: $SDj \models Ui \overset{skij}{\longleftrightarrow} SDj$,

B. DISCUSSION ON OTHER ATTACKS

An informal analysis in the following sections shows that the proposed scheme is secure against various well-known attacks, and it also provides the required functionality features. The goals G1 and G2 clearly show that Ui and SDj mutually authenticate each other with help from the GWN.

using the assumptions mentioned below:

A1. $Ui \models \#(Ti)$, $Ui \models \#(Tj)$;

A2. $GWN \models \#(Ti)$, $Ui \models \#(TGWN)$;

A3. $SDj \models \#(Ti)$, $SDj \models \#(TGWN)$, $SDj \models \#(Tj)$;

A4. $GWN \models (GWN \overset{a.P}{\longleftrightarrow} SDj)$;

A5. $SDj \models (GWN \overset{a.P}{\longleftrightarrow} SDj)$;

A6. $SDj \models GWN$ p$\Rightarrow$ $GWN \mid\sim X$;

A7. $Ui \models (Ui \overset{b.P}{\longleftrightarrow} SDj)$;

A8. $SDj \models (Ui \overset{b.P}{\longleftrightarrow} SDj)$;

The mutual authentication between Ui and SDj is as follows:

(c.P)), TGWN , Ti >i.

S1. From message 1, we get,

SDj Gh < ((Ri k Ti), ($a.P$ k $RIDj$ k Ti k $TGWN$)), $c.P$, ((Ri k Ti),$dGWN$ ($c.P$)), $TGWN$, Ti >i ($a.P$) . $GWN \longleftrightarrow SDj$

S2. Using S1, A5 and MMR, we obtain, $SDj \models GWN \mid\sim$h < ((Ri k Ti), ($a.P$ k$RIDj$ k Ti k $TGWN$)), $c.P$, ((Ri k Ti), $dGWN$ ($c.P$)), $TGWN$, Ti >i.

S3. Using S2, A3, FR and NVR, it follows that

$SDj \models GWN \models$h < ((Ri k Ti) , ($a.P$ k $RIDj$ k Ti k $TGWN$)), $c.P$, ((Ri k Ti), $dGWN$ ($c.P$)), $TGWN$, Ti >i.

S4. Using A6, S3, JR and BR, we get $SDj \models (Ri$ k$Ti)$.

S5. Using S4 and BR, we get, sk_{ij}

$SDj \models Ui \longleftrightarrow SDj$. **(Goal G2)**

S6. From message 2, we get, $skij$

Ui Gh< (($Ui \longleftrightarrow SDj$),$dSDj$($b.P$)$x$)),$Tj$ >i$Ui \longleftrightarrow b.P$ SDj.

S7. Using S6, A7 and MMR, we get,$skij$

S8. Using S7, A1, FR, NVR and BR, we get, $skij$

$Ui \models SDj \models Ui \longleftrightarrow SDj$.

S9. Using S8, A9 and JR, we get,$skij$

$Ui \models Ui \longleftrightarrow SDj$. **(Goal G1)**

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

- [39]. Hence, hash digest length is 160 bits.

- Identity ID is of length 160 bits.
- As the security of 160-bit ECC cryptosystem is equivalent to that for 1024-bit RSA cryptosystem [40] ,

VI. PERFORMANCE COMPARISON

This section presents a performance comparison of the proposed scheme with other related authentication schemes previously proposed for IoT applications. In Porambage et al.'s scheme, there are two protocols: protocol 1 allows only the legitimate members of the multicast group as eligible to continue the rest of the process of key derivation,The approximate time required for every operation and the terms used in calculating computational overhead are provided in Table 2. We use Table 2 for computational cost

TABLE 2. Approximate time required for various operations.

Notation	Description (time to compute)	Approx. computation time (seconds)
T_h	hash function	0.00032
T_{ecm}	ECC point multiplication	0.0171
T_{eca}	ECC point addition	0.0044

TABLE 5. Comparison of functionality features of the proposed scheme with related schemes.

Feature	Porambage *et al.* [36]	Porambage *et al.* [37]	Turkanovic *et al.* [38]	Our
FN_1	×	×	✓	✓
FN_2	×	✓	×	✓
FN_3	–	–	×	✓
FN_4	–	–	×	✓
FN_5	×	✓	✓	✓
FN_6	✓	×	✓	✓
FN_7	×	✓	×	✓
FN_8	×	✓	✓	✓
FN_9	×	×	✓	✓
FN_{10}	✓	✓	✓	✓
FN_{11}	✓	✓	✓	✓
FN_{12}	✓	✓	✓	✓
FN_{13}	–	–	×	✓
FN_{14}	✓	×	×	✓
FN_{15}	×	✓	✓	✓
FN_{16}	–	–	✓	✓
FN_{17}	–	×	×	✓
FN_{18}	×	×	×	✓
FN_{19}	×	×	×	✓

Note: FN_1: user anonymity property; FN_2: insider attack; FN_3: off-line password guessing attack; FN_4: stolen smart card attack; FN_5: denial-of-service attack; FN_6: known session key attack; FN_7: user impersonation attack; FN_8: man-in-the middle attack; FN_9: replay attack; FN_{10}: mutual authentication; FN_{11}: session key agreement; FN_{12}: forward secrecy; FN_{13}: stolen/lost device revocation; FN_{14}: untraceability property; FN_{15}: resilience against sensor node/sensing device capture attack; FN_{16}: GWN independent password update phase; FN_{17}: support biometric update phase; FN_{18}: provide security analysis using BAN logic; FN_{19} : provide formal security verification using AVISPA tool.
–: not applicable in a scheme; ×: insecure against a particular attack or does not support a particular feature; ✓: secure against a particular attack or supports a particular feature.

VII. CONCLUSION

We have first discussed an authentication model for future IoT applications, and then the security challenges and requirements. We have presented a new signature-based user authenticated key agreement scheme to address the security challenges and requirements in IoT. The mutual authentication between a user and an accessed sensing device is proved using the broadly-accepted BAN logic. We have also shown the security of the proposed scheme informally and the formal security verification using the widely-accepted AVISPA tool. A rigorous security analysis reveals that the proposed scheme can be protected against various known attacks by an adversary. Various network parameters are measured through a rigorous simulation using the widely-used NS2 simulator. The proposed scheme is also efficient in computation and communication, and these are comparable with other existing approaches. High security, efficient computational and communication costs along with additional functionality features show that the proposed scheme is suitable for practical applications in IoT environment as compared to other related schemes.

Acknowledgment

This paper was supported by the Sree Sowdambika College of Engineering, Final Year PG CSE student Ms.K.Ilakkya (Reg.no:921816405003) guided by Asst.Prof of Computer Science and Engineering Ms.K.Ramya. The authors thank to their colleagues for their help and support at different stages of the system development. Finally, we would like to thank the anonymous reviewers for their helpful comments.

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] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, ‘‘Internet of Things (IoT): A vision, architectural elements, and future directions,’’ Future Generat. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, 2013.

[3] D. Dolev and A. Yao, ‘‘On the security of public key protocols,’’ IEEE Trans. Inf. Theory, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[4] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, ‘‘Examining smart-card security under the threat of power analysis attacks,’’ IEEE Trans. Comput., vol. 51, no. 5, pp. 541–552, May 2002.

[5] P. Kocher, J. Jaffe, and B. Jun, ‘‘Differential power analysis,’’ in

Advances in Cryptology, vol. 1666. Berlin, Germany: Springer-Verlag, 1999, pp. 388–397.

[6] N. Koblitz, ‘‘Elliptic curves cryptosystems,’’ Math. Comput., vol. 48 , pp. 203–209, Sep. 1987.

[7] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, ‘‘DTLS based security and two-way authentication for the Internet of Things,’’ Ad Hoc Netw., vol. 11, no. 8, pp. 2710–2723, Sep. 2013.

[8] D. Liu, P. Ning, S. Zhu, and S. Jajodia, ‘‘Practical broadcast authentication in sensor networks,’’ in Proc. 2nd Annu. Int. Conf. Mobile Ubiquitous Syst. Netw. Serv. (MobiQuitous), San Diego, CA, USA, 2005, pp. 118–129.