INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 2 (2018) PAGES 2891 - 2901
RECEIVED : 25.02.2018 PUBLISHED : 23.03.2018

March 23, 2018

Signature-Based Authentication Key using BAC logic for IoT Applications

[1]S.Suba bharathi ,[2]P.Poovizhi

PG Student Communication Systems ,Assistant Professor ECE Department

Idhaya engineering college for women,chinnasalem.

Abstract

Internet of Things (IoT) is a network of all devices that can be accessed through the internet. These devices can be remotely accessed and controlled using existing network infrastructure, thus allowing a direct integration of computing systems with the physical world. This also reduces human involve-ment along with improving accuracy, efficiency and resulting in economic benefit. The devices in IoT facilitate the day to day life of people. However, IoT has an enormous threat to security and privacy due to its heterogeneous and dynamic nature. Authentication is one of the most challenging security requirements in IoT environment, where a user (external party) can directly access information from the devices, provided the mutual authentication between user and devices happens.In this paper, we present a new signature-based authenticated key establishment scheme for IoT environment. The proposed scheme is tested for security with the help of the widely-used Burrows-Abadi-Needham logic (BAN logic), informal security analysis, and also the formal security verification using the broadly-accepted Automated Validation of Internet Security Pro-tocols and Applications (AVISPA) tool. The proposed scheme is also implemented using the widely-accepted NS2 simulator, and the simulation results demonstrate the practicability of the scheme. Finally, the proposed scheme provides more functionality features, and its computational and communication costs are also comparable with other existing approaches.

Index Terms: Internet of Things (IoT), Authentication, Key establishment, BAC logic, AVISPA, NS2 simulation, Security.

1. 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 Inter-net 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 be considered as subsets of IoT [1]. The connectivity provided should be beyond machine-to-machine communication covering various protocols and applications interconnecting systems, devices and services. Multiple technologies like wireless communi-cation, embedded systems, machine learning, etc. are the building blocks of this vision.

Applications of IoT are diverse including infrastructure management in high-risk conditions, disaster management through environmental monitoring and providing remote health-care services, to list a few. IoT, while broadening access to information, has an enormous threat to security and privacy due to its heterogeneous and dynamic nature. Cyber attacks could change from virtual to physical with the increase in number of wearable devices. An estimated 50 billion objects will be a part of IoT by 2020 [2]. IoT being a relatively new concept, the security challenges involved have not been addressed appropriately at the design level for these objects. Employing effective security practices, especially authentication and key management schemes to protect anonymity and privacy, is required.

A. System Models

In this paper, we have followed two models which are discussed below.

1.IoT Authentication Model: In the given IoT authenti-cation 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 (GW Ns). Different types of users (for example, smart home user and doctor) can access the data of relevant IoT devices through the GW N. Mutual authentication between a user and a device through the GW N provides access to device data to the user [2].

2.Threat Model: We follow the widely-accepted Dolev-Yao threat (DY) model [3]. Under the DY model, communi-cation 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:

-An authentication model for IoT is presented and the security challenges involved and its requirements are discussed.

- A secure signature-based authentication and key agree-ment 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 verifi-cation 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.

C. Organization of the Paper

The paper is organized as follows. In Section II, we discuss the necessary mathematical preliminaries which are needed to describe and analyze the proposed scheme. Section III discusses some security challenges and requirements in IoT. In Section IV, we discuss some existing related work done to address these issues. Sections V and VI present the pro-posed scheme and its rigorous security analysis, respectively.

2. SECURITY CHALLENGES AND REQUIREMENTS IN IOT APPLICATIONS

As accessibility and global connectivity are the key require-ments 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 randomfailures are vulnerabilities that attackers could exploit. The various possible attacks on IoT applications are as follows: Denial-of-Service: Apart from conventional denial-of-service (DoS) attacks like exhausting resources and band-width, IoT can be susceptible to attacks on communi-cation infrastructure like channel jamming. Adversaries who are privileged insiders can gain control of the rele-vant 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:

Relevance of the data being managed by that entity. Eavesdropping: This is a passive attack through which in-formation 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 vulnerabil-ity 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. Any programming information required to deploy the solution should be communicated securely to the entities. The following are some requirements for IoT to counter security breaches:

Reliability: The aim is to guarantee information avail-ability while efficiently managing data storage. Provid-ing 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 liabil-ities must be clearly defined to avoid dages.

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 men-tioned in [7] and [8] 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 hetero-geneous network like IoT where devices and not just constraints should also be considered while developing techniques.

Safety: System components can be prone to sudden fail-ures and safety is required to reduce damage possibilities.

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

3. THE PROPOSED SCHEME

In this section, we present a new signature-based authen-ticated key establishment scheme using the 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 I. To protect thoposed scheme from strong replay attack, we use both random numbers as well as 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.

A. System Setup Phase

The system setup is done by the gateway node GW N as follows.

Step S1. GW N chooses a non-singular elliptic curve E_p over a prime finite field Z_p, p being a large prime. GW N then selects a base point P of order n over E_p such that n:P = O, where O is called the point at infinity or zero point. GW N also chooses its private key $d_{GW\ N}$ and computes the corresponding public key $Q_{GW\ N} = d_{GW\ N}$:P .

Step S2. GW N then chooses a collision-resistant one-way cryptographic hash function h( ).

Step S3. For biometric authentication, GW N uses the following two fuzzy extractor functions:

Gen: It is a probabilistic generation function that takes as input the user personal biometrics Bio_i, and returns $_i$ 2 f0; 1g^l that is the biometric key of length l bits and $_i$ that is a public reproduction parameter.

Rep: It is a deterministic function to be used during authentication. The input is the user biometrics, say Bio^0 and $_i$, provided the hamming distance between Bio^0 and the original previously entered biometrics Bio_i is less than t, where t is an error tolerance threshold value. The output is the original biometric key $_i$, that is,

$_i$ =Rep($Bio^0{}_i$; $_i$).

Step S4. Finally, the system parameters fE_p(a; b); p; P; h( ); $Q_{GW\ N}$; Gen( ); Rep( ); tg are made public, whereas $d_{GW\ N}$ is kept secret by GW N

B. Sensing Device Registration Phase

All the sensing devices in IoT are registered offline by the GW N as follows.

Step SD1. For each device SD_j, the GW N chooses a unique identity ID_j and a unique private key d_j, and calculates the corresponding public key $Q_j = d_j$:P . It further computes RID_j = h(ID_j k d_j).

Step SD2. The GW N pre-loads fID_j; d_j; RID_jg in the memory of SD_j. Furthermore, the GW N stores fID_j; RID_j; Q_jg in its database, and then makes Q_j as public.

C. User Registration Phase

D. A user U_i registers with the GW N by executing the following steps:

E.

F. Step R1. U_i chooses a unique ID_i, a unique private key d_i and calculates the corresponding public key Q_i =

G. d_i:P . U_i sends registration request message with $RID_i = h(ID_i\ k\ d_i)$ to GW N via a secure channel.

H. Step R2. GW N computes $R_i = h(RID_i\ k\ d_{GW\ N}\ )$, stores it on smart card SC_i and sends it to U_i via a secure channel.

I. Step R3. U_i selects a password P W_i and imprints the biometrics template Bio_i at the sensor of a specific terminal. SC_i then computes the following:

J.

K. $Gen(Bio_i) = (\ _i;\ _i)$;

L. RP W_i = $h(P\ W_i\ k\ d_i\ k\ ID_i\ k\ _i)$;

M. $R_i = R_i$ $h(ID_i\ k\ P\ W_i\ k\ _i)$;

N. $d_i = d_i$ $h(ID_i\ k\ _i)$:

O. Step R4. U_i stores fd_i ; RP W_i; Gen( ); Rep( ); $_i$; h( ); tg and replaces R_i with R_i in SC_i. In addition, U_i also makes Q_i public.

P.

Q. D. Login Phase

R.

S. U_i executes the following steps to login to the GW N:

T. Step L1. After inserting SC_i, U_i enters his/her identity ID_i^0 and password P W_i^0, and also imprints biometrics $Bio^0{}_i$ at the sensor of a specific terminal.

U. Step L2. SC_i then computes $_i{}^0 = Rep(Bio^0{}_i;\ _i)$, $d^0{}_i = d_i\ h(ID_i^0\ _i{}^0)$ and RP $W_i^0 = h(P\ W_i^0\ k\ ID_i^0\ k\ d^0{}_i\ k\ _i{}^0)$, and checks if RP W_i^0 = RP W_i holds.

V. Step L3. If the above condition is verified successfully, U_i chooses a random secret number a 2 Z_p , generates the current timestamp T_i and creates a login message with signature as follows:

W. where ID_j is the identity of the sensing device SD_j that U_i wants to communicate with. U_i finally sends $fDID_i^0$; DID_j^0; A_i; T_i; r_i; s_ig to GW N as login message via a public channel.

X. E. Authentication and Key Agreement Phase

Y.

Z. In this phase, the GW N validates U_i and helps in estab-lishing a session key between an accessed sensing device SD_j and a legal user U_i with the help of the following steps:

AA. Step A1. After receiving the login message from U_i at the time T_i^0, the GW N first checks the validity of timestamp by the condition $T_i^0\ \ T_i\ \ \ T$. If it is valid, the GW N then calculates $N_{GW\ N} = d_{GW\ N} :A_i =((N_{GW\ N}\ )_x; (N_{GW\ N}\ )_y)$, $RID_i = DID_i^0\ \ (N_{GW\ N}\ )_y$,

BB.

CC. $ID_j = DID_j^0\ (N_{GW\ N}\ )_y$, $R_i = h(RID_i\ k\ d_{GW\ N}\ )$, $V_i = h(ID_j\ k\ T_i\ k\ N_{GW\ N}\ k\ R_i)$.

DD.

EE. The GW N checks if ID_j is registered with it. If it is, then the GW N verifies U_i's signature as follow

FF. $N_i = ((N_i\ )_x; (N_i\ )_y)$

GG.

HH. $= (u_{GW\ N} :P + t_{GW\ N} :Q_i)d_{GW\ N}$:

II.
JJ. Note that ($u_{GW N}$:P +$t_{GW N}$:Q_i) $d_{GW N}$ = (((V_i P)=s_i)
KK. +((($r_i d_i$):P)=s_i)) $d_{GW N}$ = (1=s_i) (V_i +$r_i d_i$) $d_{GW N}$:P
LL.
MM. = (1=s_i)(as_i) $d_{GW N}$:P = a:$Q_{GW N}$ = N_i = ((N_i)$_x$; (N_i)$_y$). GW N checks if r_i = (N_i)$_x$ = (N_i)$_x$ = r_i as explained above to verify U_i's signature.
NN. Step A2. After successful signature verification, GW N chooses a random secret number c 2 Z_p , generates its current timestamp $T_{GW N}$ and computes the following message with signature:
OO.
PP. $C_{GW N}$ = c:P = (($C_{GW N}$)$_x$; ($C_{GW N}$)$_y$);
QQ. F. Password and Biometric Update Phase
RR.
SS. U_i executes this phase internally without involving the

GW N to reduce overhead as follows:

Step PB1. U_i enters his/her identity ID_i, current pass-word P W_i^{old} and imprints current biometrics $Bio^{old}{}_i$ at the sensor of a specific terminal. SC_i then computes

SC_i checks if RP W_i^{old} = RP W_i and the request is terminated if the verification is not successful.

Step PB2. U_i then enters new password P W_i^{new} and imprints new biometric $Bio^{new}{}_i$. SC_i computes the fol-lowing:

Step PB3. RP W_i, d_i , R_i and $_i$ on SC_i are replaced with RP W_i^{new}, (d_i)^{new}, (R_i)^{new} and $_i^{new}$, respec-tively.

G. Smart Card Revocation Phase

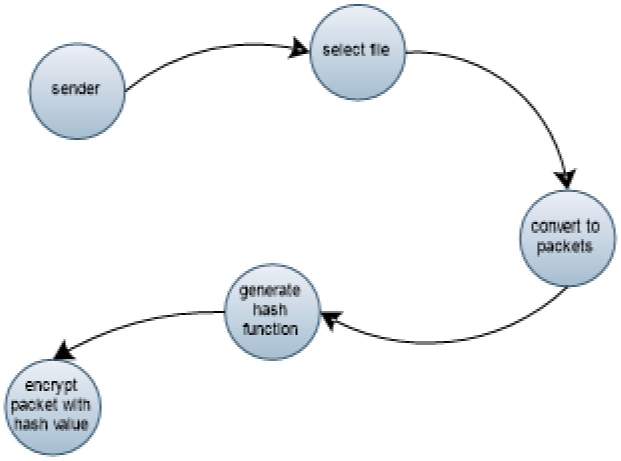
If the smart card SC_i of a legitimate user U_i is lost, the following steps can be executed for requesting a new one:

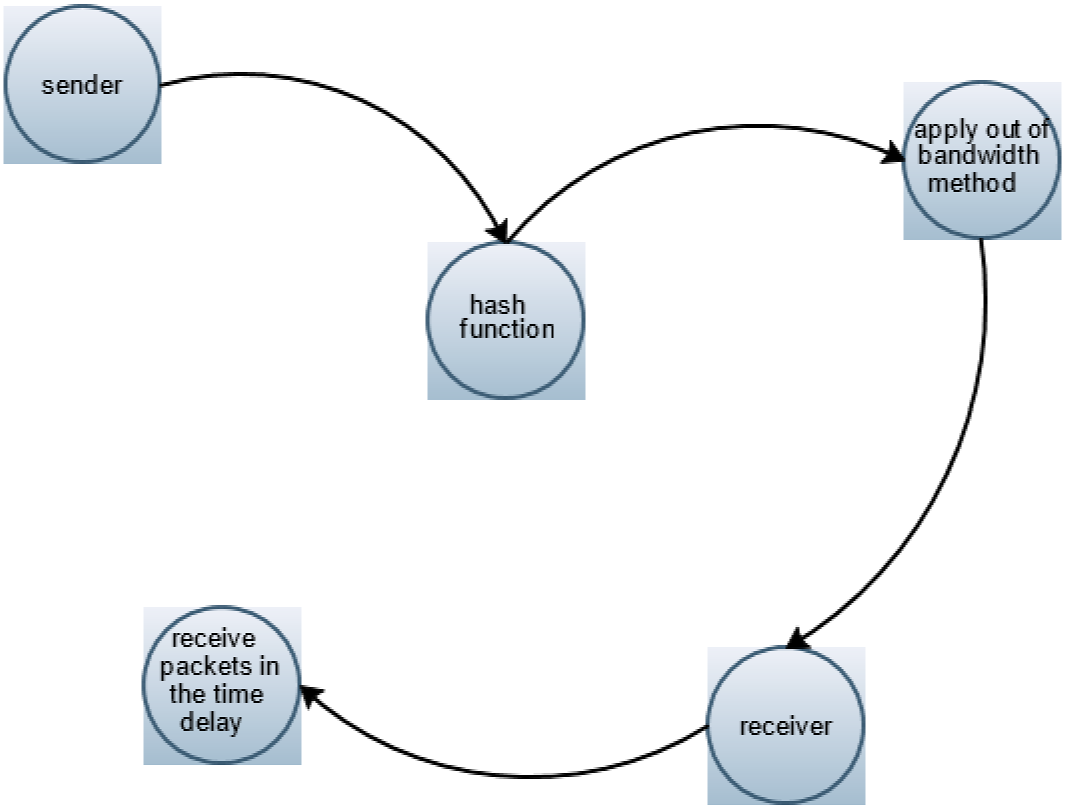
Step RV1. U_i creates a registration request message with the same ID_i and new private key $d^{new}{}_i$ as RID_i^{new} = h($d^{new}{}_i$ k ID_i) and sends it to the GW N via a secure channel

4. PROPOSED MODULES:

BAC Generation:

The sender side, the authentication information—BAC—is generated based on a selected hash function with the packet content and a commonly agreed key as the input. Based on the value of each bit (0/1) of BAC, some packets are scheduled to be sent out with additional delays.

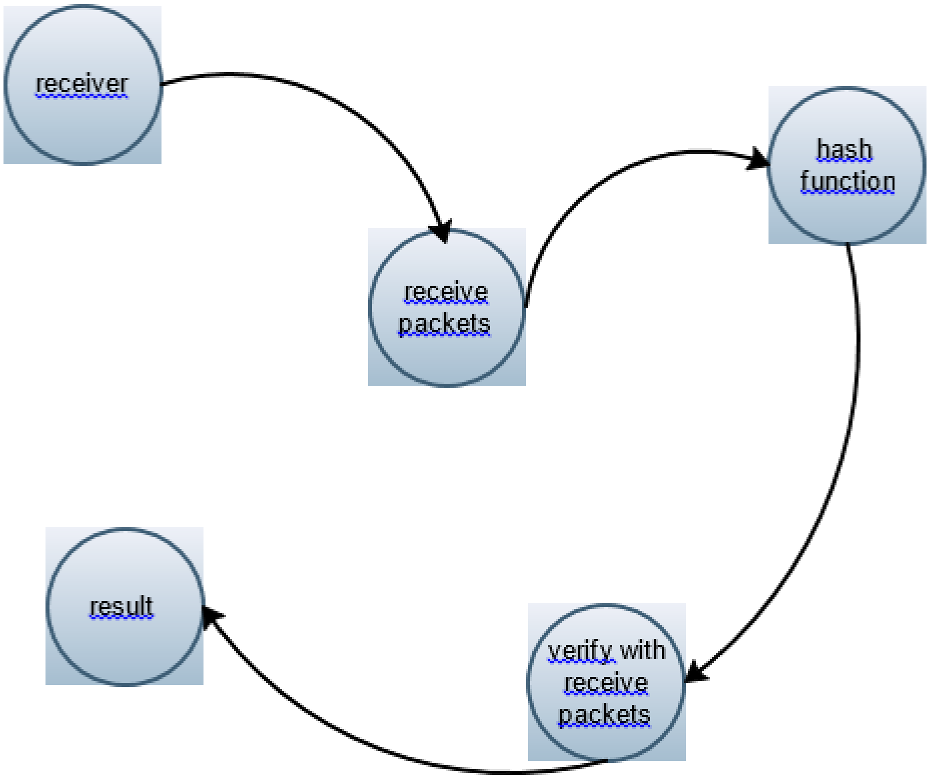



sender
hash function
apply out of bandwidth method
receiver
receive packets in the time delay

BAC Embedding

With the extracted BAC bits and received data packets, the receiver applies the same hash function (H) on the received data packets with the same secret key (k) to generate the content-based BAC following the same procedure used for BAC generation at the sender side. Then, the extracted BAC is compared with the generated BAC.

The comparisons consist of two parts: the first part is on the first n bits, while the second is on the rest f 0 bits.



5. PRACTICAL PERSPECTIVE: NS2 SIMULATION STUDY

In this section, we simulate our scheme using the widely-accepted network simulation tool, NS2 2.35 simulator [41] on Ubuntu 14.04 LTS platform to measure the network performance parameters, such as throughput (in bps) and end-to-end delay (in seconds) to show the impact of the scheme.

A. Simulation Parameters

The details of the parameters used in NS2 simulation are provided in Table VI. The network simulation time is taken as 1800 seconds (30 minutes). Both static and dynamic (mobile) types of users are considered in simulations. The speeds of the mobile users are considered as 2, 10 and 15 mps, respectively. Apart from these, all other standard parameters are taken for NS2 simulations.

B. Simulation Environment

Three different network scenarios are used.For all the scenarios, we have taken one GW N and 50 SD_js.

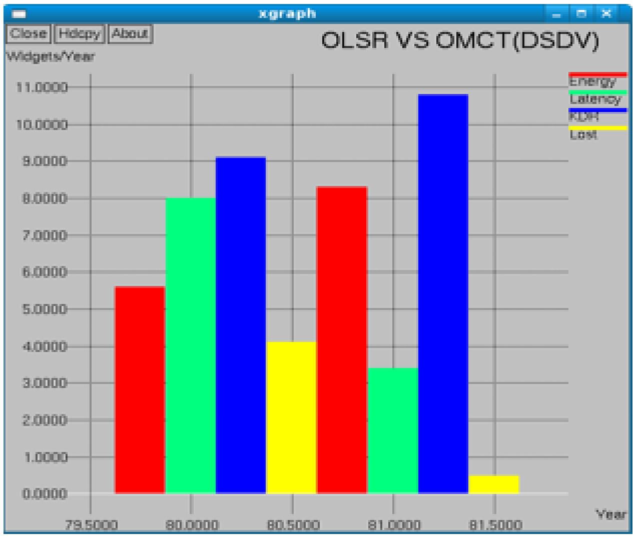
Scenario 1. This scenario has three users (U_is): one is static and other two are moving with the speeds of 2 mps and 15 mps, respectively.

Scenario 2. This scenario has five users (U_is): two are static and other three are moving with the speeds of 2 mps, 15 mps and 15 mps, respectively.

Scenario 3. This scenario has eight users (U_is): four are static and other four are moving with the speeds of 2 mps, 2 mps, 10 mps and 15 mps, respectively.

Moreover, we assume that the hash output (if we use SHA-1 hash algorithm) and the identity have bit lengths 160 bits and 160 bits, respectively.

SIMULATION RESULTS AND DISCUSSIONS



CONCLUSION

I have first discussed an authentication model for future IoT applications, and then the security challenges and requirements. I have presented a new signature-based 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. I 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.

REFERENCES

[1] L. Atzori, A. Iera, and G. orabito, “The Internet of Things: A survey,” Computer Networks, vol. 54, no. 15, pp. 2787 – 2805, 2010.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, no. 7, pp. 1645 – 1660, 2013.

[3] D. Dolev and A. Yao, “On the security of public key protocols,” IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208, 1983.

[4] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, “Examining smart-card security under the threat of power analysis attacks,” IEEE Transactions on Computers, vol. 51, no. 5, pp. 541–552, 2002.

[5] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in 19th Annual IACR Crypto Conference (Advances in Cryptology) - CRYPTO’99, ser. Lecture Notes in Computer Science, vol. 1666, Santa Barbara, California, USA, 1999, pp. 388–397.

[6] N. Koblitz, “Elliptic Curves Cryptosystems,” Mathematics of Computation, vol. 48, pp. 203–209, 1987.

[7] T. Kothmayr, C. Schmitt, W. Hu, M. Brnig, and G. Carle, “DTLS based security and two-way authentication for the Internet of Things,” Ad Hoc Networks, vol. 11, no. 8, pp. 2710 – 2723, 2013.

[8] D. Liu, P. Ning, S. Zhu, and S. Jajodia, “Practical broadcast authentication in sensor networks,” in 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2005), San Diego, California, USA, 2005, pp. 118–129.

[9] X. Cao, W. Kou, L. Dang, and B. Zhao, “IMBAS: Identity-based multiuser broadcast authentication in wireless sensor networks,” Computer Communications, vol. 31, no. 4, pp. 659 – 667, 2008.