A Secure and Light Weight Authentication Protocol for Wireless Sensor Network in Internet of Things

Mrunula Sarvabhatla  Lakshmi Narayana K  Chandra Sekhar Vorugunti
M.Tech-CSE,First year  Asst prof- CSE  Dhirubhai Ambani Institute of ICT
N.B.K.R-IST-Nellore, A.P  SITAMS-Chittoor, A.P  Gandhinagar-382007, Gujarat
mrudula.s911@gmail.com  kodavali.lakshmi@gmail.com  vorugunti_chandra_sekhar@daiict.ac.in

ABSTRACT
With the advancement of cloud and Internet of Things (IoT) technology, mobile phones, RFID systems and wireless sensor networks can be integrated to form heterogeneous systems to execute smarter applications. However, data exchange between remote cloud and sensor node via internet poses critical security challenges. The major challenge is the authentication and key exchange among the communication agents. In addition, resource constrained devices such as RFID tags, sensors in WSN and IoT integration (WSNIT) would require robust and light weight authentication schemes. To combat these issues we establish in this paper a first of its kind of a WSN security protocol in IoT, which is light weight and resistant to cryptographic attacks.

Categories and Subject Descriptors

General Terms
Security

Keywords

1. INTRODUCTION
Wireless sensor networks (WSN) offer a virtual digital layer which senses the critical information from the physical world and submit it to storage system for remote processing and data analysis. Internet of Things (IoT) results in embedding of computational competence in all kinds of resource constrained devices like RFID tags, mobile devices etc. and allows these devices to connect to WSN and access the critical data stored in the sensors.

2. MOTIVATION AND PROBLEM STATEMENT
The amalgamation of IoT and WSN (WSNIT) [1,2,3] is in a promising stage and industry giants like IBM, H.P has started initial research on WSNIT. In china, IBM developed a smarter app called ‘A Smarter Planet’, which is built on top of sensors to deliver reliable Internet-based information from intelligent water management system and weather forecast systems to farmer’s mobiles through Internet (SMS).

In order to allow safe exchange of critical data between WSNIT and various online social networks and to link the aggregated data from sensor nodes with web services based on SOAP, demands for stringent authentication system that is robust and light weight. Hence, we intent to come up with a light weight and cryptographic attack resistant authentication scheme in order to reap the maximum benefits from WSNIT.

3. WSNIT SYSTEM
As shown the fig 1, the data from sensors of WSN which is deployed in real time applications is transmitted to remote cloud servers via middle servers comprises of internet, computing and processing resources.

3.1 Communication Agents of WSNIT
WSNIT consists of three communication entities i.e. remote Cloud (C), middle server (M) and WSN (S) having identities IDc, IDm and IDs respectively. During the initialization stage of the system, C and M shares a symmetric key ‘m’ and M and S share ‘k’ securely. Cloud and Middle server are private and not accessible to outside world. The WSN and middle server exchanges data via public Internet. Due to the space restrictions, we are elucidating the protocol diagrammatically. The protocol runs from top to bottom and from left to right.

Figure 1. Graphical view of WSNIT.
4. WSNIT Authentication Protocol

Cloud (C) | Middle Server (M) | WSN (S)
---|---|---
Generate a random number \( R_c \)

\[ \{ R_c \} \]

Computes: \( M_1 = R_c \oplus h(ID_c \oplus ID_m \oplus k) \)

\[ \{ M_1 \} \]

Computes:
\( R_c = M_1 \oplus h(ID_c \oplus ID_m \oplus k) \)
\( R_2 = R_c \oplus h(k \oplus R_c \oplus ID_c \oplus ID_m) \)
\( M_2 = h(ID_c \oplus ID_m \oplus R_c \oplus R_c \oplus k) \)

\[ \{ M_2, R_2 \} \]

Computes: \( R_c^* = R_2 \oplus h(k \oplus R_c \oplus ID_c \oplus ID_m) \)
\( M_2^* = h(ID_c \oplus ID_m \oplus R_c \oplus R_c \oplus k) \)

Check \( M_2^* = M_2, M \) Authenticates S

Generate \( R_m \)
\( M_3 = h(ID_c \oplus R_m \oplus R_m \oplus R_c) \)
\( R_3 = R_c \oplus h(R_c \oplus ID_m \oplus k) \)
\( R_4 = R_c \oplus h(R_c \oplus R_c \oplus ID_m \oplus k) \)

\[ \{ M_2, M_3, R_3, R_4 \} \]

Computes:
\( R_m^* = R_3 \oplus h(R_c \oplus ID_m \oplus k) \)
\( M_3^* = R_4 \oplus h(R_c \oplus R_c \oplus ID_m \oplus k) \)
\( M_2^* = h(ID_c \oplus ID_m \oplus R_c \oplus R_c \oplus k) \)

If \( M_2^* = M_2 \) and \( M_3^* = M_3, C \) authenticates M and S.

Generates a session key S.K.
\( M_4 = h(ID_c \oplus R_m \oplus m) \oplus S.K \)
\( M_5 = h(ID_c \oplus m) \oplus S.K \oplus \| R_m^* \) \( M_6 = h(ID_c \oplus k \oplus R_c^* \) \oplus S.K \)
\( M_7 = h(ID_c \| k \| S.K \| R_c^*) \)

\[ \{ M_4, M_5, M_6, M_7 \} \]

\( S.K^* = M_4 \oplus h(ID_c \oplus R_m \oplus m), M_5^* = h(ID_c \| m \| S.K \| R_m^*) \)

If \( M_5^* = M_5, C \) is authenticated by M.

\[ \{ M_6, M_7 \} \]

\( S.K^* = M_6 \oplus h(ID_c \| k \| R_c), M_7^* = h(ID_c \| k \| S.K \| R_c) \)

If \( M_7^* = M_7, C \) is authenticated by S.

5. SECURITY ANALYSIS

Table 1. Equations or Parameters available to an attacker

<table>
<thead>
<tr>
<th>Equation Accessible to an Attacker (E) via internet.</th>
<th>Values known to ‘E’</th>
<th>Values not known to ‘E’</th>
</tr>
</thead>
<tbody>
<tr>
<td>( M_1 = R_c \oplus h(ID_c \oplus ID_m \oplus k) )</td>
<td>None</td>
<td>( ID_c, ID_m, k )</td>
</tr>
<tr>
<td>( M_2 = h(ID_c \oplus ID_m \oplus R_c \oplus R_c \oplus k) )</td>
<td>None</td>
<td>( ID_m, ID_c, R_c, k )</td>
</tr>
<tr>
<td>( R_2 = R_c \oplus h(k \oplus R_c \oplus ID_c \oplus ID_m) )</td>
<td>None</td>
<td>( ID_c, ID_m, R_c, k )</td>
</tr>
<tr>
<td>( M_6 = h(ID_c \oplus k \oplus R_c \oplus S.K) )</td>
<td>None</td>
<td>( ID_c, R_c, k )</td>
</tr>
<tr>
<td>( M_7 = h(ID_c | k | S.K | R_c) )</td>
<td>None</td>
<td>( ID_c, S.K, K, R_c )</td>
</tr>
</tbody>
</table>

In our proposed scheme, the keys shared among C,M and S i.e k, m are assumed to be shared securely and it is impossible for an attacker ‘E’ to intercept. As shown in the table, even though the symmetric keys k and m are leaked out, in order to perform impersonation, MiM attacks, ‘E’ requires one or more 128 bits long random numbers and identities i.e \( ID_c, ID_m, ID_c, R_c, R_s, S.K \). It is computationally impossible for ‘E’ to guess these values in real polynomial time. Therefore, we can conclude that, our scheme resists all major cryptographic attacks.

6. CONCLUSION

In this manuscript, we have proposed and analyzed first of its kind of secure and light weight authentication protocol for the amalgamation of WSN and IoT. We have designed the scheme using only light weight hash (SHA-2) and XOR operations. As shown in table 1 and discussed earlier, our scheme is attack resistant, due to the fact that, the attacker must guess one or more unknown variables of 128 bit length (which is computationally impossible) to succeed in any attack.

7. REFERENCES

