Body Sensor Network-Care
A Secure IoT-Based Modern Healthcare System Using Body Sensor Network

Presented by Ranjan Mohan.
What is BSN?

Body Sensor Network (BSN), also known as Body Area Network is a collection of sensor nodes that are:
- Low-powered
- Lightweight
- Wireless

Function:
- Monitor Human body functions
- Monitor Surrounding Environment

Placement
- Inside the body (Invasive)
- Outside the body (Non-invasive)
Need for BSN

- A recent report from United Nations predicts that by 2050, the population would comprise of 2 billion older people (about 22% of the world population)
- About 80% of aged people older than 65 suffer from at least one chronic disease.

Note: By 2050, WE would comprise of the aged population.

So technically, the seeds we plant in development would benefit us directly.
Role of IoT in this Scenario?

- **Internet of Things (IoT)**
  - Conglomeration of devices that are connected to the internet.
  - Not restricted to usual Desktop PCs, Laptops or Mobile phones

- With the advent of IoT, it is possible to achieve seamless interactions among different devices - medical sensors, monitoring cameras, home appliances, etc.

- That is, building a Bio Technology combined with IoT would enable us to mimic
  - a medical assistant watching over the vitals
  - help with medicinal intakes and so on,
  just by installing a small device on the patient.
An insight into existing systems

Recent wireless healthcare research and projects have aimed at monitoring the patients at various levels:

- Continuous
- In-ambulatory
- In-clinic
- Open Environment (Athletic health monitoring)

The following slides brief recent work on this domain.
CodeBlue

- Healthcare Research Project developed at Harvard Sensor Network Lab
- Wireless sensors placed on the patient’s body transmit data to their authorized devices.
- Any doctor/medical professional who requests for this medical info queries using their own personal device.
- Focuses more on robust scalable communication with less focus towards security.
Alarm-net

- Patient health monitoring project based on heterogeneous networks, developed at the University of Virginia.
- Consists of body sensors and environment sensors.
- Facilitates network and data security for physiological, environment and behavioural parameters about residents.
- Recent research proves that this design is susceptible to adversarial confidentiality attacks.
UbiMon

- BSN based healthcare system proposed by Department of Computing, Imperial College, London.
- No consideration of security as a requirement in this model.
MobiCare

- Wide area mobile patient monitoring system developed by Chakravorty.
- Security requirement acknowledged and worked on, but not sufficient for real-time healthcare applications.
- Need to be addressed:
  - Secure Localization
  - Anonymity
  - etc
Patient monitoring during disaster events developed at John Hopkins University.

Comprises of multiple physiological monitors to collect health information (blood oxygenation, pulse rate etc).

The author acknowledged the need for encryption but did not specify the scheme to ensure confidentiality.
Need to work further?

- All projects focus on:
  - Reliability
  - Cost Effectiveness
  - Power Consumption

- Most of them only address the requirement for security and privacy, That is why!
Why Secure it?

- What’s at stake?
  - Patient’s medical data,
  - Patient’s identification,
  - Potential control over the Patient.

The following slides elucidate some key issues/ potential weak-links to the system that need to be addressed.
Data Privacy

- Necessary to protect the data from disclosure.
- Sensors collect and forward sensitive data to a PDA/ coordinator.
- Possible to eavesdrop and tap crucial data.
Data Integrity

- Adversary could alter data being exchanged by tampering with packets - corrupting or even appending extra redundant data.

- Lack of integrity could disregard a critical condition and deem healthy or even alter a healthy record to indicate as critical.
Data Freshness

The receiver should be able to accept only fresh data and should discard and log any replay attacks.

Anonymity

A packet being transmitted from/to a patient should not contain any deducible information regarding the source or destination of a packet.
Secure Localization

- Patient location could be modified by altering signal strengths which would indicate a change in proximity to the actual patient location.
- Such tampering/loss of location integrity should be identified.

Authentication

- The sender and receiver should be mutually authenticated to avoid compromise at both ends.
BSN Care - A secure IoT based health care proposal

- Focuses on data from a person wearing multiple biosensors
- This data is sent to a Local Processing Unit (LPU) which is a user held device (Phone, Tablet, PDA etc)
- This LPU analyzes the data and depending on the requirement, it contacts one or multiple of the following through the BSN-Care Server
  - Family members
  - Local Physician
  - Emergency Unit
- The LPU unit sends reading updates to the BSN-Care server periodically
BSN-Care Server

- The LPU unit sends reading updates to the BSN-Care server periodically

- This server maintains an action table based on received data.

- Based on the action table it takes appropriate response based on the incoming sensor data
### Action Table Example

<table>
<thead>
<tr>
<th>BSN BP Data</th>
<th>Action</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>BP ≤ 120</td>
<td>No Action</td>
<td>Null</td>
</tr>
<tr>
<td>BP &gt; 130</td>
<td>Inform Family Members</td>
<td>FR:T/F</td>
</tr>
<tr>
<td>BP &gt; 160 and FR:F</td>
<td>Inform Local Physician</td>
<td>PR:T/F</td>
</tr>
<tr>
<td>BP &gt; 160, FR:F and PR:F</td>
<td>Inform Emergency</td>
<td>ER:T/F</td>
</tr>
</tbody>
</table>

*FR:* Family Response; *PR:* Physician Response; *ER:* Emergency Response
Reinforcing the Security

To meet the stated security requirements we use:

- Lightweight Anonymous Authentication Protocol
  To achieve NetSec requirements

- OCB Authenticated Encryption Mode
  To achieve data security requirements
Lightweight Anonymous Authentication Protocol

This protocol is implemented as follows:

- **Phase 1 - Registration Phase**
  
  BSN-Care Server issues security credentials to LPU through a secure channel

- **Phase 2 - Anonymous Authentication Phase**
  
  Mutual authentication before data transmission
## Notations used

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>( L )</td>
<td>Local processing unit (LPU)</td>
</tr>
<tr>
<td>( S )</td>
<td>BSN-Care server</td>
</tr>
<tr>
<td>( ID_L )</td>
<td>Identity of the LPU</td>
</tr>
<tr>
<td>( AID_L )</td>
<td>One-time-alias identity of the LPU</td>
</tr>
<tr>
<td>( SID )</td>
<td>Shadow identity of the LPU</td>
</tr>
<tr>
<td>( K_{ls} )</td>
<td>Shared key between the LPU and the server</td>
</tr>
<tr>
<td>( K_{em} )</td>
<td>Shared emergency key between the LPU and the server</td>
</tr>
<tr>
<td>( Tr_{Seq} )</td>
<td>Track sequence number</td>
</tr>
<tr>
<td>( LAI )</td>
<td>Location area identifier</td>
</tr>
<tr>
<td>( h(.) )</td>
<td>One-way hash function</td>
</tr>
<tr>
<td>( \oplus )</td>
<td>Exclusive-OR operation</td>
</tr>
<tr>
<td>( | )</td>
<td>Concatenation operation</td>
</tr>
</tbody>
</table>
Phase 1

Each corresponding to a particular Shadow ID
Phase 2

\[ \text{Generate: } N_i \]
\[ \text{Compute: } \]
\[ N_z = K_{ls} \oplus N_i \]
\[ AID_z = h(ID_L \| K_{ls} \| N_i \| Tr_{seq}) \]
\[ EL = LAI_1 \oplus h(K_{ls} \| N_i) \]
\[ V_1 = h(N_i \| LAI_1 \| K_{ls}) \]
\[ \text{or} \]
\[ sid_j \in SID, k_{em_j} \in K_{em} \]
\[ AID_z = sid_j \oplus K_{ls} = k_{em_j} \]

\[ \mathbf{M}_{A_1} : \{ AID_L, N_x, Tr_{seq} \text{ (if req.)}, EL, V_1 \} \]

\[ \text{Check: } ? \ Tr_{seq} \]
\[ \text{Get: } N_i = K_{ls} \oplus N_z, \]
\[ LAI_1 = EL \oplus h(K_{ls} \| N_i) \]
\[ \text{Compute and Verify: } \]
\[ ? V_1, ? AID_L, ? LAI_1 \text{ (If req.)} \]
\[ \text{Generate: } m \]
\[ \text{Compute: } Tr_{seq_{serv}} = m \]
\[ Tr = h(K_{ls} \| ID_L \| N_i) \oplus Tr_{seq_{serv}} \]
\[ V_2 = h(Tr \| K_{ls} \| ID_L \| N_i) \]

\[ \mathbf{M}_{A_2} : \{ Tr, V_2, x \text{ (If req.)} \} \]

\[ \text{Compute and Verify: } V_2^* = h(Tr \| K_{ls} \| ID_L \| N_i) = V_2 \]
\[ \text{Compute and Update: } \]
\[ Tr_{seq_{serv}} = h(K_{ls} \| ID_L \| N_i) \oplus Tr \]
\[ K_{t_{serv}} = h(K_{ls} \| ID_L \| Tr_{seq_{serv}}) \]
\[ Tr_{seq} = Tr_{seq_{serv}} \oplus K_{tl} = K_{t_{serv}} \]
\[ \text{or} \]
\[ K_{tl} = h(ID_L \| k_{em_j}) \oplus x, K_{ls} = K_{t_{serv}} \]

\[ K_{t_{serv}} = K_{tl_{serv}} \]

\[ K_{ls} = K_{t_{serv}} \]
Evaluation

Security Perspective

- In contrast to AES-CBC and CBC-MAC used in Alarm-net and Median. This OCB-based data security approach provides:
  - Less computational overhead
  - Anonymity
  - Secure Localization

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SR1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SR2</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SR3</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SR4</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SR5</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Evaluation (Contd)

Performance Perspective

- AES-OCB and AES-CBC tested using Java Cryptographic Extension (LCE)
- LPU Specifications
  - HTC Desire
  - 0.72 GHz ARM A-8
  - Li-ion 1230 mAh
  - Android 2.2
Evaluation (Contd)
Conclusion

After a thorough survey of existing work and intensive research a BSN system has been proposed to counter all the security related problems faced by existing deployments without compromise in performance and scalability.
References

- David Malan, Thaddeus Fulford-Jones, Matt Welsh and Steve Moulton - CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care
- Images were taken from the paper or internet, I do not own the rights =)