Key Exchange Protocol for Wireless Sensor Network: Formal Verification using CSN Modal Logic

Yue Li & Dr. Thomas Newe
Department of Electronic and Computer Engineering
University of Limerick,
Limerick, Ireland

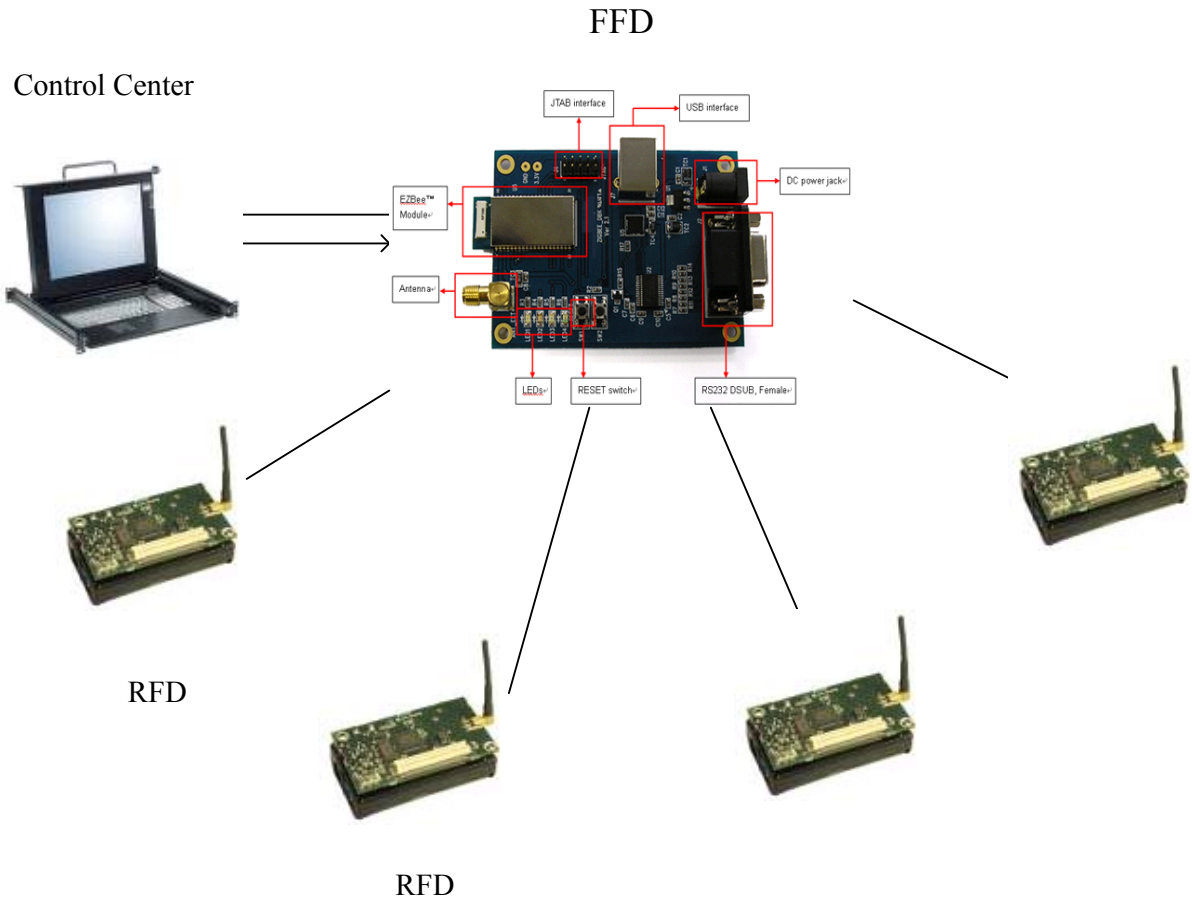
UNIVERSITY of LIMERICK
OLLSCOIL LUIMNIGH

SENSORS APPLICATIONS SYMPOSIUM

Outline

- Security issues in wireless sensor networks.
- Introduction of key exchange protocol.
- Discussion of the hybrid authenticated key exchange protocol.
- Introduction of formal verification and the Coffey-Saidha-Newe (CSN) modal logic
- Formal verification of the hybrid authenticated key exchange protocol using the CSN modal logic.
- Modifications to the protocol.
- Future work and conclusion

Wireless Sensor Networks (WSNs)



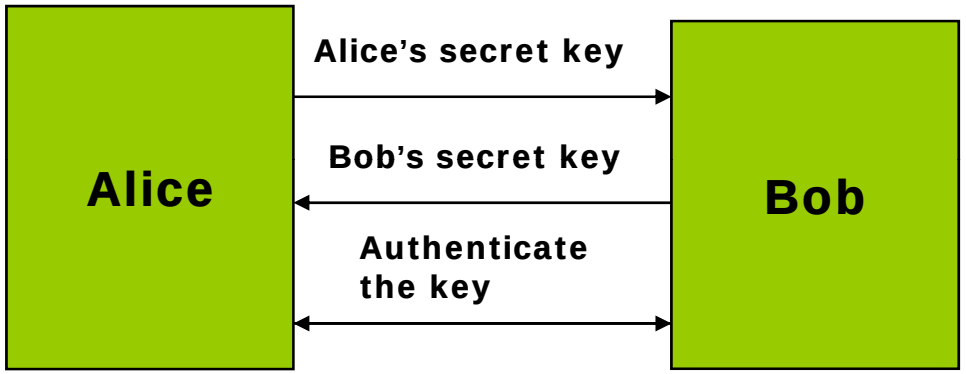
Security in Wireless Sensor Networks (WSNs)

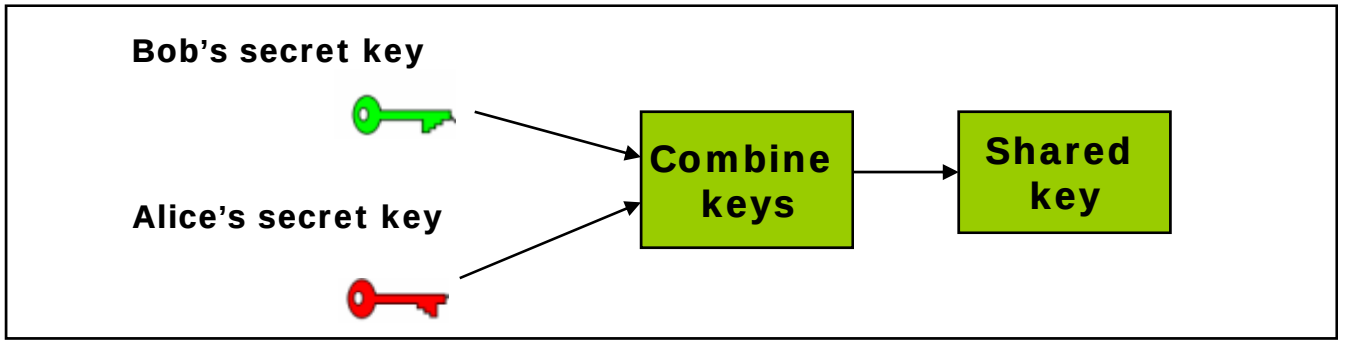
- WSNs applications have gained in popularity
  - Habitat monitoring
  - Health application
  - Environment monitoring
- Data is of high privacy for some particular applications
- Secure communication system is essential

Challenges:

- Sensor devices are resource constrained;
  - Low processing capability
  - Low power supply

Key exchange protocol





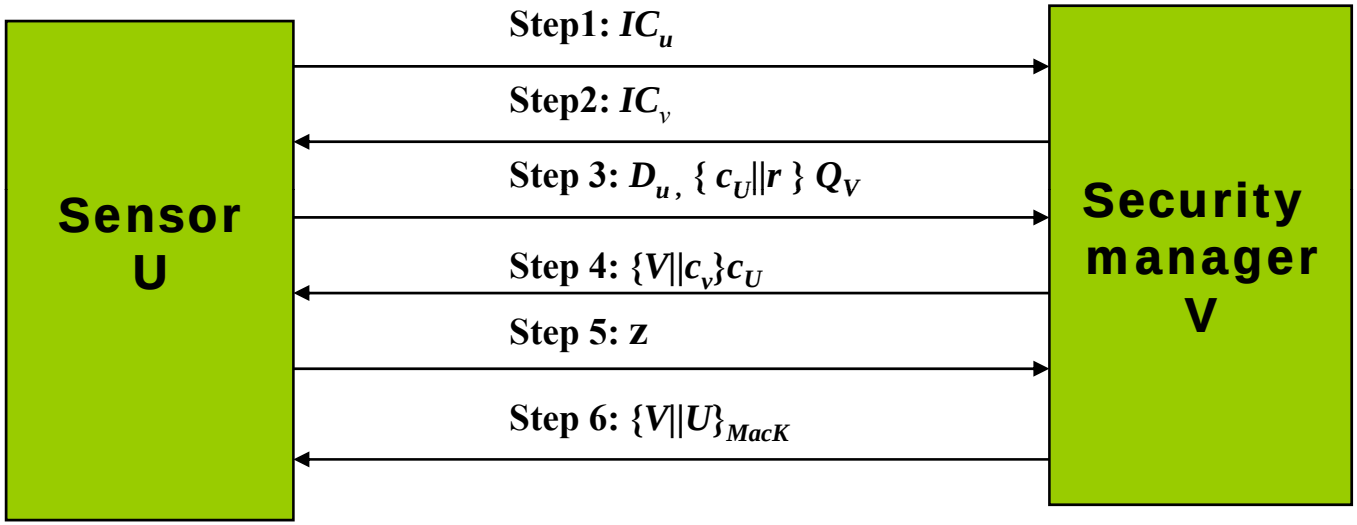
Hybrid key exchange protocol

- Huang et al. proposed a hybrid authenticated key exchange scheme, which is based on a combination of elliptic curve cryptography (ECC) and symmetric-key operations.
- It puts the computing burden on security manager where the resources are less constrained.
- The hybrid scheme reduces the high cost public-key operations at the sensor side and replaces them with efficient symmetric-key based operations
- The scheme authenticates the two identities based on elliptic curve implicit certificates

Hybrid key exchange protocol propose by Huang et al.

- Notations and System parameters
  - H(): denotes a secure one-way hash function which maps finite binary strings to integers in the range [2,n-2].
  - KDF(): denotes secure key derivation function,
  - MAC(): denotes a message authentication code function
  - ||:denotes the conventional binary string concatenation operator.
  - (q_U, Q_U): denote the private/public pair of sensor U, where q_U is a random integer and $Q_U = q_U P$, also $q_U = Q_U^{-1}$
  - IC_U: denotes the implicit certificate of sensor U.

Hybrid key exchange protocol.



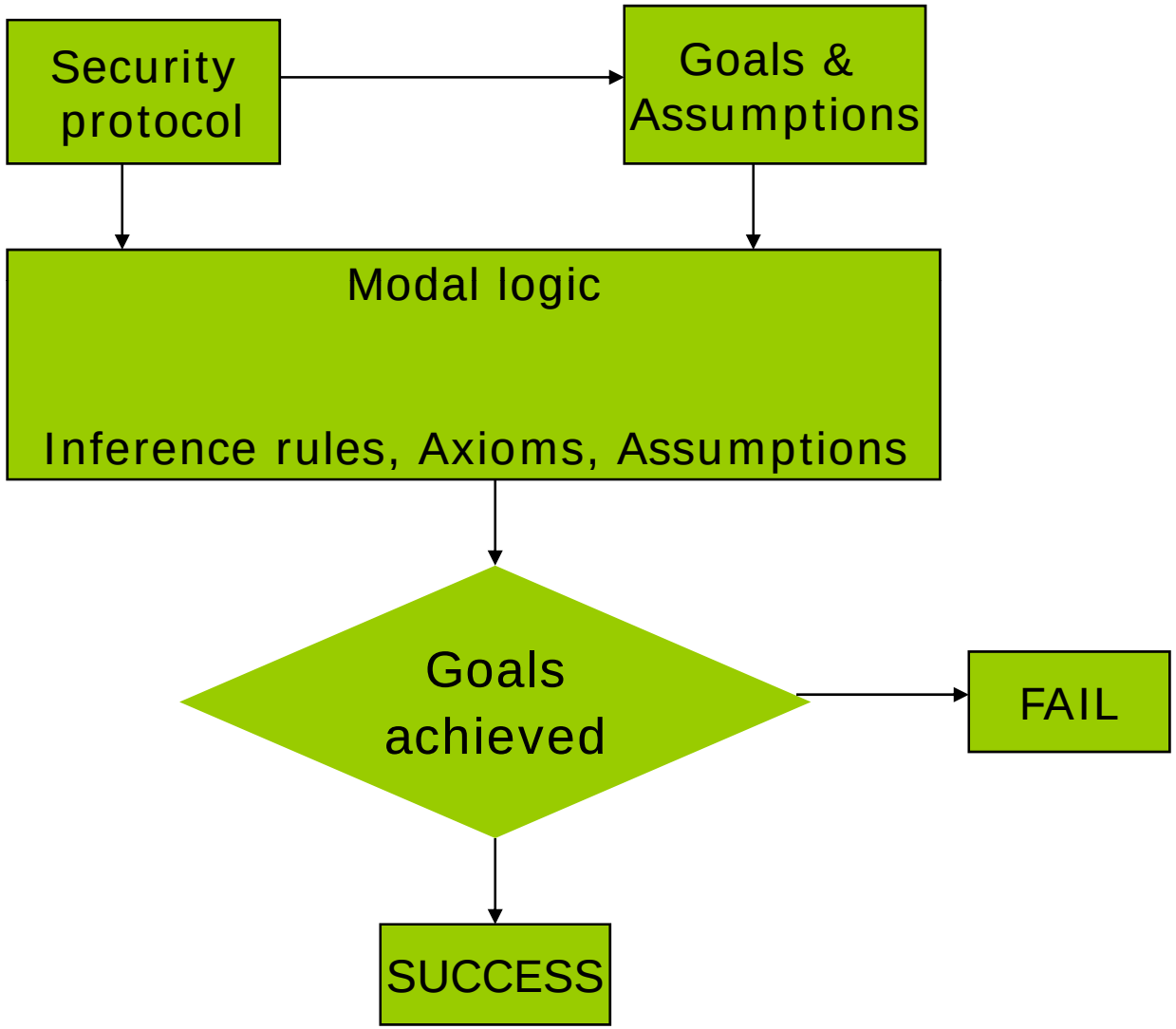
- $Q_U=H(IC_U)B_U+Q_{CA}$;
- $MacK \,||\, SessionK \leftarrow KDF(c_U||c_V\,||U||V\,)$
- $z = q_U H(MacK) + d_U \bmod n$

- At step 3, U randomly picks a k-bit integer c_U and a $(160-k)$-bit integer r, computes $d_U \leftarrow H(c_U||r)$, $D_U = d_U P$, $R = d_U Q_V$;

Formal Verification Logic

- Cryptographic protocols were normally analyzed by informal reasoning.
- Formal methods can also be implemented to find subtle flaws in security protocols.
- Some Logics are developed, they could express and deduce security properties.
- One of the most important formal approaches for security protocol verification is modeling and verifying the protocol using modal logics developed for the analysis of knowledge and belief.

Flow chart of formal verification using modal logics



The Coffey-Saidha-Newe (CSN) Formal Logic

- Analyze both knowledge and belief, addressing issues of both security and trust.
- Is capable of verifying hybrid cryptographic protocols.
- Inferences are provided for natural deduction
- Axioms are used to express the fundamental properties of both public key and symmetric cryptographic protocols

The Coffey-Saidha-Newe (CSN) Formal Logic

Some examples of CSN logic and Axioms

$$\exists t \exists x \exists i, i \in \{ENT\}(L_{i,t}x \wedge L_{i,t}ks_{(\Sigma,\Psi)} \rightarrow L_{i,t}(E(x, ks_{(\Sigma,\Psi)}))$$

If some entity *i* knows and can reproduce *x* at time *t* and entity *i* knows and can reproduce the shared secret key of the two parties then *i* can encrypt message *x* using the shared secret key between the two parties at time *t*

Formal analysis of the key exchange protocol

- In order to formally verify the hybrid key exchange protocol one must first list:
  - The Goals

    &
  - Initial Assumptions of the protocol.

Goals of the hybrid key exchange protocol

- **Goal 1: $K_{V,t3}(\exists t, t<t3, S(U,t,(D_U, c_u||r))$**

Goal 1 indicates that the security manager *V* will receive a message contain the ephemeral public key, D_U before the end of step 3. The message also includes the link key contribution c_U and value *r*

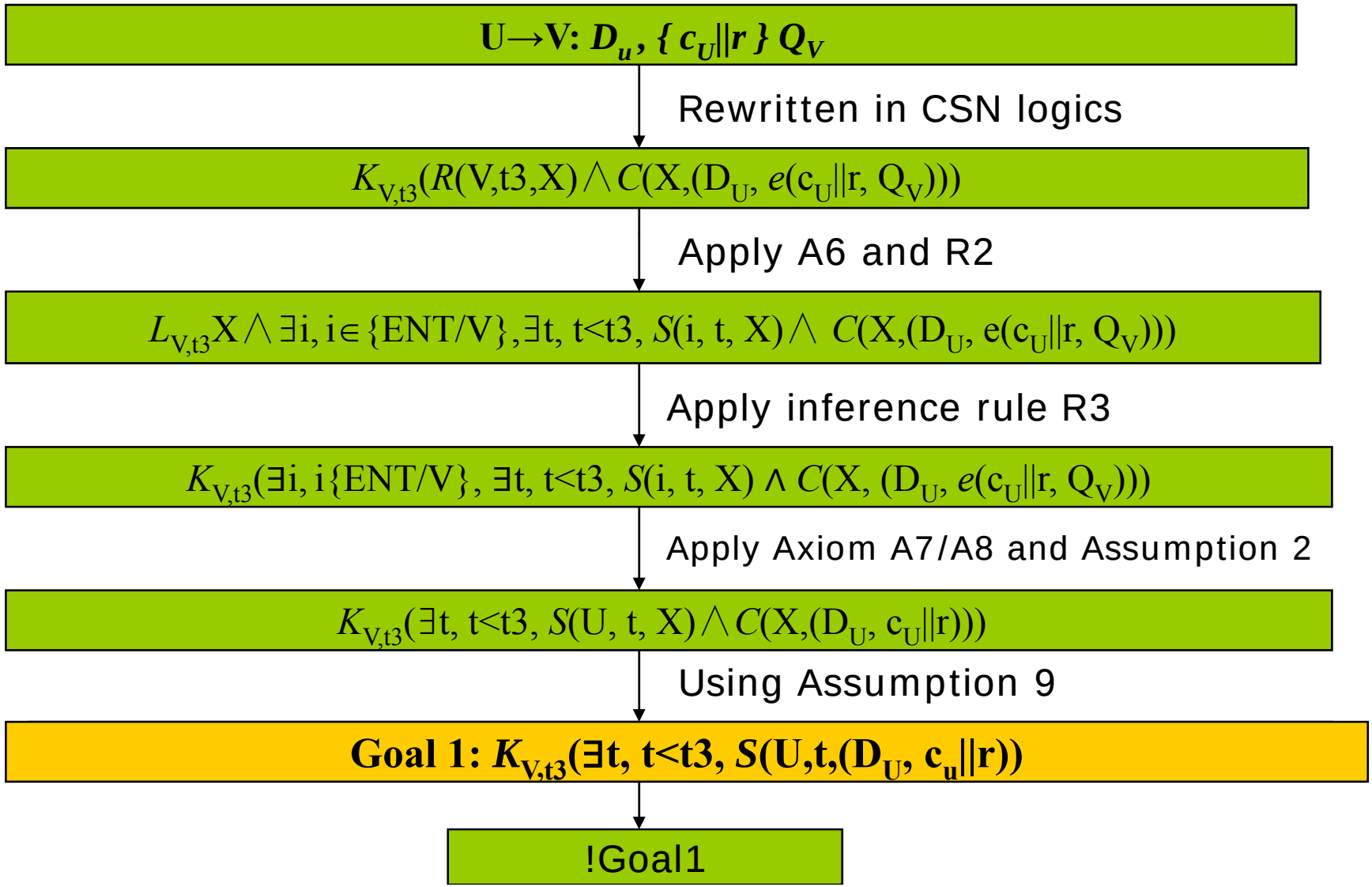
- **Goal 2: $K_{U,t4}(\exists t, t3<t<t4, S(V, t, X) \wedge C(X,V||c_v))$**

Goal 2 states that sensor *U* will receive message $(V||c_V)$ from security manager *V* before the end of step 4 but after step 3.

Initial assumptions of the hybrid key exchange protocol

- 1: $\forall i, i \in \{ENT\}, \forall t,\ t1<t<t_U, L_{i,t}IC_U \wedge L_{i,t}Q_U$
- 2: $\forall i, i \in \{ENT\}, \forall t,\ t2<t<t_V, L_{i',t}IC_V \wedge L_{i',t}Q_V$
- 3: $\forall i, i \in \{ENT\}, L_{i,t}U \wedge L_{i,t}V$
- 4: $L_{U,t0}D_u \wedge K_{U,t0}(\forall i, i \in \{ENT/U\}, \forall t, t<t3, \neg L_{i,t}D_u)$
- 5: $L_{U,t0}c_U \wedge K_{U,t0}(\forall i, i \in \{ENT/U\}, \forall t, t<t3, \neg L_{i,t}c_u) \rightarrow (c_U \in KS_{\{U,V\}})$
- 6: $L_{V,t0}c_V \wedge K_{V,t0}(\forall i, i \in \{ENT/V\}, \forall t, t<t4, \neg L_{i,t}c_V)$
- 7: $\forall i, I \in \{U,V\}, \forall t, t>t3, L_{i,t}(c_U \| r) \wedge L_{i,t}(c_U \| r \rightarrow d_U)$
- 8: $L_{V,t0}MacK \wedge K_{V,t0}(\forall i, i\{ENT/V\}, \forall t, t<t4, \neg L_{i,t}MacK) \rightarrow (MacK \in KS_{\{U,V\}})$
- 9: $B_{V,t0}(t, t<t5, S(U, t, X) \wedge C(X,(D_U, c_U \| r))$

Flow chart of the formal analysis



Summary of the formal verification

- Goal 1 has not been proved. Although the security manager *V* believes the identity of the sensor *U* after step 3, no knowledge is gained without proper authentication of the sensor *U*.

- Neither Goal 3 nor Goal 4 can be proved as the security manager only has belief that private key Q_U^{-1} is only known to its rightful owner, sensor node *U,* no knowledge is gained, however knowledge is required for total security

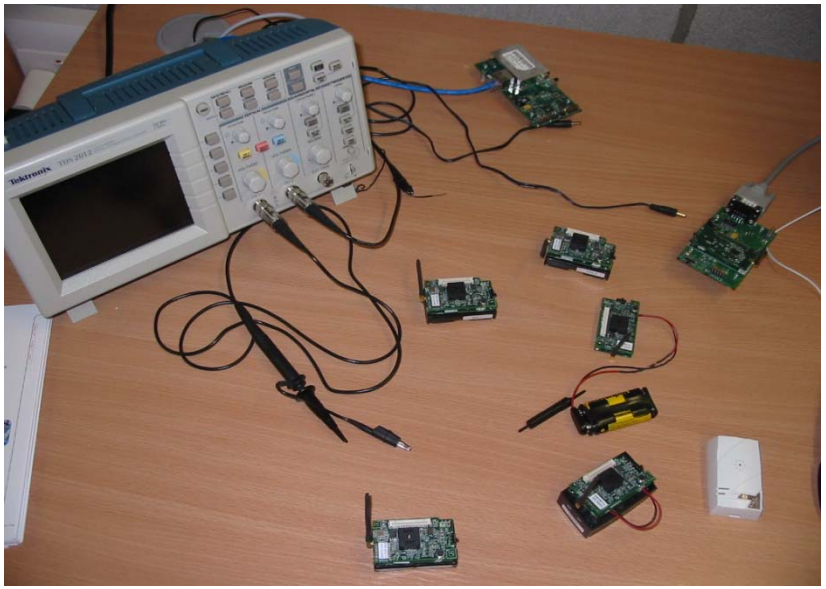
Modifications to the protocol

Step 1: $U \rightarrow V$: IC_U
Step 2: $V \rightarrow U$: IC_V
Step 3: $U \rightarrow V$: $Enc_V\{U, c_U||r\}, Sig_U\{c_U||r\}$
Step 4: $V \rightarrow U$: $\{V||c_v, r\}k_{cu}$
Step 5: $U \rightarrow V$: $\{U||V, r\}MacK$

- The modified protocol completes the initial session key setup in five rounds rather than the six rounds in original protocol
- The computation complexity is little bit higher, as one modular multiplication is required to compute public key encryptions at sensor side at step 3
- The modification to the protocol is to allow the authentication of the sensor *U* by the security manager *V* to take place at the start of the protocol. This prevents the protocol from impersonation attack in the early stage of the protocol.

Future work

- Further investigation on existing key establishment protocols for WSNs
- Improve and optimise the new modified key exchange protocol
- A formal verification of the improved protocol will need to be completed to prevent further protocol weaknesses.
- Implementation and evaluation of the new protocol on wireless sensor nodes will be applied.



Conclusion

- A hybrid authenticated key exchange (AKE) protocol for wireless sensor network and the CSN formal verification logic is discussed.
- The formal verification of the hybrid AKE protocol using the CSN modal logic is presented.
- The analysis shows that the protocol has security weaknesses in authentication of identities of sensor nodes.
- A proposed modification to the protocol to correct this weakness was presented.
- Future work was presented.

Q&A

Thank you for your attention!