Trust Establishment in Ad Hoc and Sensor Networks

Efthimia Aivaloglou, Stefanos Gritzalis, Charalabos Skianis

{eaiv, sgritz, cskianis}@aegean.gr

University of the Aegean

Sensor Networks for CIIs

- Sensor networks
  - Composed of small, resource constrained sensor nodes spread over sensing fields
  - A special case of ad hoc networks: cooperative behaviour, distributed control, dynamically changing topologies
- Sensor Networks used for Critical Information Infrastructures
  - For the provision of context-rich services
  - For their protection

Securing Sensor Networks

- Basic security requirements
  - Confidentiality and integrity
  - Authentication and access control
  - Secure routing, secure node grouping
  - Secure information aggregation
  - Intrusion detection
- Trust management in Sensor Networks
  - For representing trust evidence, evaluating and maintaining in-network trust relationships based on rules and policies
  - For dealing with selfish or malicious node behaviour
  - As the basis for other security services

Trust Establishment Frameworks for Ad Hoc and Sensor Networks: Requirements

Ad Hoc and SNs Characteristics	Requirements and Constraints
Lack of fixed infrastructure and centralised management points	Support for distributed, cooperative trust evaluation, without trusted intermediaries like TTPs
Dynamically changing topology and membership, wireless communications	No stable hierarchies of trust relationships. Flexibility to membership changes Support for uncertain trust evidence.
Susceptibility to node misbehavior	Support for controlled trust revocation Protection from bad mouthing attacks Incentives for cooperation on trust evaluation.
Constrained energy and computation capabilities	Acceptable resource consumption
Pre-deployment knowledge may be available	Support for pre-established and stable trust relationships.

Trust Establishment Frameworks for Ad Hoc and Sensor Networks: Categorisation

- Certificate-based frameworks
  - Trust decisions based on certificate validity assessment
  - A valid certificate proves that the holder is trusted either by a CA or by other trusted nodes
  - Proactive frameworks
- Behaviour-based frameworks
  - Trust relationships between neighbouring nodes formed through continuous monitoring
  - Reactive frameworks

Certificate-Based Frameworks (1)

- Hierarchical Trust Frameworks

  [Verma et al. (2001)], [Davis (2004)]

  - Trust represented by certificates signed by offline TTPs
  - Certificate revocation either by TTP or collaboratively
- Distributed Trust Frameworks

  [Hubaux et al. (2001)]

  - Trust relationships modelled as a trust graph, shared between the network nodes
  - Trust evaluated using certificate chains
- Distributed Certification Authority Frameworks

  [Zhou and Haas (1999)], [Yi and Kravets (2003)]

  - Secret sharing mechanisms to distribute CA functionality to an aggregation of nodes

Certificate-Based Frameworks (2)

	Parties Involved	Considerations
Hierarchical Trust Frameworks	i, j, n offline CAs	Availability of CAs, Scalability
Distributed Trust Frameworks	i, j	Certificate Revocation, Accountability
Distributed CA Frameworks	i, j, t partial CAs	Deployment Complexity, Communication and computation requirements

Behaviour-Based Frameworks

- Trust viewed as the level of positive cooperation between neighbouring nodes
- Trust evaluated both independently and cooperatively
  - *Direct trust* calculated according to the direct experience the trustor may have on the trustee.

    Network traffic monitoring and intrusion detection mechanisms are used.

    Indirect trust derived using recommendations about the trustee from other nodes.

    Node reputation spread through the network, enabling the formation of a connected trust graph.

Behaviour-Based Frameworks – Direct Trust

- Frameworks may include the evidence collection mechanisms and direct trust evaluation formulas to be used
- Parameters used for the evaluation of the direct trust:
  - Results from network traffic monitoring mechanisms (NTM)
  - Raw sensing data consistency (RDC)
  - Black lists (BL)
  - Weighted combination on event significance (WCS)
  - Freshness as a weight factor for the events (FWF)

	NTM	RDC	BL	WCS	FWF
Yan et al. (2003)	+		+		
Pirzada and McDonald (2004)	+			+	
Theodorakopoulos and Baras (2004)	+				
Ganeriwal and Srivastava (2004)	+	+			+
Virendra et al. (2005)	+				

Behaviour-Based Frameworks – Indirect Trust

- Several formalisations for the evaluation of the indirect trust value through combining recommendations
- Parameters used for the evaluation of the indirect trust:
  - Recommendations from other nodes, usually being their direct trust values to the target (R)
  - Confidence factors assigned to the recommendations from the source nodes (CFR)
  - Weights for the combination of the recommendations according to the trust values of the issuer for the source nodes (WCR)

	R	CFR	WCR
Yan et al. (2003)	+		
Pirzada and McDonald (2004)			
Theodorakopoulos and Baras (2004)	+	+	+
Ganeriwal and Srivastava (2004)	+		+
Virendra et al. (2005)	+		+

Behaviour-Based Frameworks – Concerns

- Node willingness to share recommendations is crucial
- Pre-established and stable trust relationships not supported
- The evaluation of direct trust is a continuous process
- Applicability for the case of sensor networks

Comparative Evaluation – Supported Trust Characteristics

- Support for uncertain evidence (UC)
- Transitivity (T)
- Trust revocation (R)

	UC	T	R
Verma et al. (2001)	U		C, I
Davis (2004)	U		C, I
Hubaux et al. (2001)	C	U	
Zhou and Haas (1999)	U		
Yi and Kravets (2003)	U		C, I
Yan et al. (2003)	U	U	U, G/I
Pirzada and McDonald (2004)	U		U, G
Theodorakopoulos and Baras (2004)	C	C	U, G
Ganeriwal and Srivastava (2004)	U	C	C, G
Virendra et al. (2005)	U	C	U, G

C: Controlled, U: Uncontrolled, G: Gradual, I: Immediate

Comparative Evaluation – Memory Requirements

	L	M	H
Verma et al. (2001)		+	
Davis (2004)			+
Hubaux et al. (2001)			+
Zhou and Haas (1999)		+	
Yi and Kravets (2003)			+
Yan et al. (2003)		+	
Pirzada and McDonald (2004)		+	
Theodorakopoulos and Baras (2004)	+		
Ganeriwal and Srivastava (2004)	+		
Virendra et al. (2005)			+

Comparative Evaluation – Computational Requirements

	L	M	H
Verma et al. (2001)		+	
Davis (2004)			+
Hubaux et al. (2001)			+
Zhou and Haas (1999)			+
Yi and Kravets (2003)			+
Yan et al. (2003)		+	
Pirzada and McDonald (2004)	+		
Theodorakopoulos and Baras (2004)		+	
Ganeriwal and Srivastava (2004)		+	
Virendra et al. (2005)		+	

Comparative Evaluation – Communication Requirements

	L	M	H
Verma et al. (2001)			+
Davis (2004)			+
Hubaux et al. (2001)		+	
Zhou and Haas (1999)			+
Yi and Kravets (2003)			+
Yan et al. (2003)		+	
Pirzada and McDonald (2004)	+		
Theodorakopoulos and Baras (2004)		+	
Ganeriwal and Srivastava (2004)		+	
Virendra et al. (2005)		+	

Comparative Evaluation – Required Pre-Configuration

	L	M	H
Verma et al. (2001)		+	
Davis (2004)		+	
Hubaux et al. (2001)		+	
Zhou and Haas (1999)			+
Yi and Kravets (2003)			+
Yan et al. (2003)		+	
Pirzada and McDonald (2004)	+		
Theodorakopoulos and Baras (2004)	+		
Ganeriwal and Srivastava (2004)	+		
Virendra et al. (2005)	+		

Final Remarks

- Applicability for the case of sensor networks
  - Computational complexity for certificate-based frameworks
  - Energy requirements of behaviour-based frameworks
- Increased sophistication → Increased complexity and resource consumption
- Two approaches in the representation and evaluation of trust:

  Not alternative, but supplementary

Questions