Epistemic Logic Based on Dolev-Yao Model

Mario R. F. Benevides, Luiz C. F. Fernandez, Anna C. C. M. de Oliveira

[1]Instituto de Matemática e Programa de Engenharia de Sistemas e Computação
COPPE - Universidade Federal do Rio de Janeiro (UFRJ) – Rio de Janeiro, RJ – Brazil

{mario,lcfernandez,acoliveira}@cos.ufrj.br

Abstract. *In this work, we extend multi-agent epistemic logic for reasoning about properties in protocols. It is based on Dolev-Yao model and uses structured propositions, a new technique to deal with messages, keys and properties in security protocols in an uniform manner, keeping the logic propositional. In order to illustrate the applicability of this new logic, an example is presented.*

1. Introduction

There are many approaches to formally verify authenticity and secrecy in communication protocols. In this work we are most interested in logical approaches to deal with that kind of system, in particular based on [Dolev and Yao 1983].

Epistemic logics deal with concepts like knowledge and believes. Many of theses logics have been tailored to be applied to computer science problems. They have a semantics based on [Lamport 1978] and can be used for protocol verification.

Some approaches use epistemic logic for reasoning about protocol specifications [Cohen and Dam 2007, Boureanu et al. 2009, Kramer 2008]. The most important feature that differentiate our approach is the use of structured propositions, i.e., these are propositions that have some kind of inner structure. Allowing for the development of a new technique to deal with security protocols in an uniform way, keeping the logic propositional.

In section 2 we present the Dolev-Yao model. Section 3 introduces the Dolev-Yao multi-agent epistemic logic and section 4 provides some future works and final remarks.

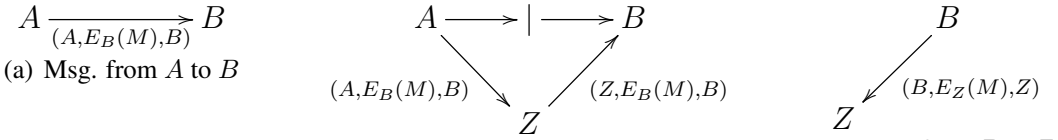
2. Dolev-Yao Model

Introduced in [Dolev and Yao 1983], this is a seminal work in this area. They work with symmetric public key protocols and consider a perfect encryption, i.e., the keys used are unbreakable. We present the system followed by examples and rules that can be obtained.

2.1. Public Key Protocols

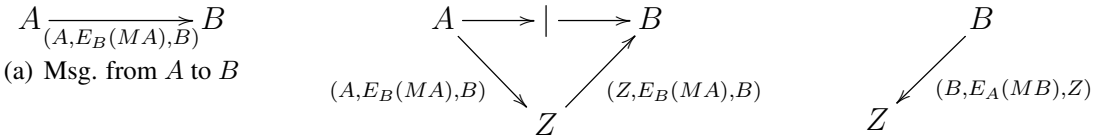
We assume that every user X in network has an encryption function E_X (public) and a decryption function D_X (known only by X). The requirements are: $E_X D_X(M) = D_X E_X(M) = M$; and for any user Y knowing $E_X(M)$ does not reveal anything about M. In this model, we are reasoning about the intruder knowledge, where the intruder is a user who wants to obtain the content of other users' communication.

Example 1 *A sends message M to B [Fig. 1(a)]; intruder Z intercepts this message and sends message $(Z, E_B(M), B)$ to B [Fig. 1(b)]; B sends message $(B, E_Z(M), Z)$ to Z [Fig. 1(c)], Z decodes $E_Z(M)$ and obtains M.*



(a) Msg. from A to B (b) Intruder Z's actions (c) Msg. from B to Z

Figure 1. Illustration of Example 1.



(a) Msg. from A to B (b) Intruder Z's actions (c) Msg. from B to Z

Figure 2. Illustration of Example 2.

Example 2 *A sends message MA to B and B replies to the user that is encrypted with the message M and not to the sender [Fig. 2(a)]; intruder Z intercepts this message and sends message $(Z, E_B(MA), B)$ to B [Fig. 2(b)]; B sends message $(B, E_A(MB), Z)$ to Z [Fig. 2(c)] and Z **cannot** decode $E_A(MB)$ to obtain M.*

2.2. Rules

These rules are not presented in the original paper, but they can easily be obtained from the theory presented there. Here, we are assuming a set $\mathcal{K} = \{K_1, \dots\}$ of keys, a set T represent a intruder knowledge and an encryption function $\{M\}_K$, which encrypt a message M under key K. A user can only decrypt an encrypted message $\{M\}_K$ if he knows the key K.

Reflexivity: $\dfrac{M \in T}{T \vdash M}$ *Encryption:* $\dfrac{T \vdash K \quad T \vdash M}{T \vdash \{M\}_K}$ *Decryption:* $\dfrac{T \vdash \{M\}_K \quad T \vdash K}{T \vdash M}$

Pair-Composition: $\dfrac{T \vdash M \quad T \vdash N}{T \vdash (M, N)}$ *Pair-Decomposition:* $\dfrac{T \vdash (M, N)}{T \vdash M} \quad \dfrac{T \vdash (M, N)}{T \vdash N}$

3. Dolev-Yao Multi-Agent Epistemic Logic

This section presents the Dolev-Yao multi-agent epistemic logic $\mathbf{S5_{DY}}$. It is aimed to reasoning about knowledge in protocols, i.e., *keys*, *messages*, *encryption/decryption*, *agents* and so on. We propose this new semantics and an axiomatization for this logic.

3.1. Language and Semantics

There is a novelty in the language of $\mathbf{S5_{DY}}$, formulas are built from expressions and not only from proposition symbols. Intuitively, an expression is any peace of information that can be encrypted, decrypted or concatenated in order to be communicated.

Definition 1 *The Dolev-Yao multi-agent epistemic language consists of a set Φ of countably many proposition symbols, a finite set $\mathcal{A}$ of agents, a set of keys $\mathcal{K} = \{k_1, \dots\}$, the boolean connectives $\neg$ and $\wedge$, a modality K_a for each agent a[1]. The expressions and formulas are defined as follows:*

[1]We use the standard abbreviations $\bot \equiv \neg\top$, $\varphi \vee \phi \equiv \neg(\neg\varphi \wedge \neg\phi)$, $\varphi \rightarrow \phi \equiv \neg(\varphi \wedge \neg\phi)$ and $B_a\varphi \equiv \neg K_a \neg\varphi$.

$$E ::= p \mid k \mid (E_1, E_2) \mid \{E\}_k, \textit{ where } k \in \mathcal{K}.$$
$$\varphi ::= e \mid \top \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid K_a\varphi, \textit{ where } e \in E,\ a \in \mathcal{A}.$$

Definition 2 *A multi-agent epistemic* frame *is a tuple $\mathcal{F} = (S, \sim_a)$ where:*

- *S is a non-empty set of states;*
- *$\sim_a$ is a reflexive, transitive and symmetric binary relation over S, for each $a \in \mathcal{A}$.*

Definition 3 *A multi-agent epistemic* model *is a pair $\mathcal{M} = (\mathcal{F}, V)$, where $\mathcal{F}$ is a frame and V is a valuation function $V : E \to 2^S$ satisfying the following conditions:*

1. $V(m) \cap V(k) \subseteq V(\{m\}_k)$
2. $V(\{m\}_k) \cap V(k) \subseteq V(m)$
3. $V(m) \cap V(n) = V((m, n))$

We call a rooted multi-agent epistemic model $(\mathcal{M}, s)$ an epistemic state. Condition 1 ensures that, in any state, if we have a message m and a key k, then we must have the encrypted message $\{m\}_k$. Condition 2 establishes that if we have a encrypted message $\{m\}_k$ and a key k, then we must be able to decrypt it and obtain m. Condition 3 says that in any state, we have messages m and n iff we have the pair (m, n).

Definition 4 *Let $\mathcal{M} = \langle S, \sim_a, V\rangle$ be a multi-agent epistemic model. The notion of satisfaction $\mathcal{M}, s \models \varphi$ is defined as follows:*

- *$\mathcal{M}, s \models e$ iff $s \in V(e)$*
- *$\mathcal{M}, s \models \neg\phi$ iff $\mathcal{M}, s \not\models \phi$*
- *$\mathcal{M}, s \models \phi \wedge \psi$ iff $\mathcal{M}, s \models \phi$ and $\mathcal{M}, s \models \psi$*
- *$\mathcal{M}, s \models K_a\phi$ iff for all $s' \in S$, if $s \sim_a s'$ then $\mathcal{M}, s' \models \phi$*

3.2. Axiomatization

1. *All instantiations of propositional tautologies*,
2. $K_a(\varphi \to \psi) \to (K_a\varphi \to K_a\psi)$,
3. $K_a\varphi \to \varphi$,
4. $K_a\varphi \to K_aK_a\varphi$ (+ *introspection*),
5. $\neg K_a\varphi \to K_a\neg K_a\varphi$ (– *introspection*),
6. $K_am \wedge K_ak \to K_a\{m\}_k$ (*encryption*),
7. $K_a\{m\}_k \wedge K_ak \to K_am$ (*decryption*),
8. $K_am \wedge K_an \leftrightarrow K_a(m, n)$ (*pair composition & decomposition*).

Inference Rules - **M.P.**: $\varphi, \varphi \to \psi/\psi$; **U.G.**: $\varphi/K_a\varphi$; **Sub.**: $\varphi/\sigma\varphi$ [2]

Theorem 1 $\mathbf{S5_{DY}}$ *is sound and complete w.r.t. the class of* $\mathbf{S5_{DY}}$ *models.* □

Example 3 *Returning to example 1. We have three agents: A, B and Z. We assume that $k_{XY} = k_{YX}$ for every agent X and Y.*

[2] Where σ is a map uniformly substituting formulas for propositional variables. Axioms 1-5 are standard in literature [Fagin et al. 1995]. Axioms 6-8 enforces the semantical properties of the valuation function, i.e., conditions of definition 3.

0. $KB_0 = \{K_A k_{AB},\ K_B k_{AB},\ K_B k_{BZ},\ K_Z k_{BZ},\ K_A m\}$ *initial knowledge*

$\overset{send_{AB}(\{m\}_{k_{AB}})\downarrow}{---}$

$\overset{Z\ intecepts\downarrow}{---}$

1. $KB_1 := KB_0 \cup K_Z\{m\}_{k_{AB}}$

$\overset{send_{ZB}(\{m\}_{k_{AB}})\downarrow}{---}$

2. $KB_2 := KB_1 \cup K_B\{m\}_{k_{AB}}$

$K_B m$ $ax.\ 7$

$K_B\{m\}_{k_{ZB}}$ $ax.\ 6$

$\overset{send_{BZ}(\{m\}_{k_{BZ}})\downarrow}{---}$

3. $KB_3 := KB_2 \cup K_Z\{m\}_{k_{BZ}}$

$K_Z m$ $ax.\ 7$

Intruder Z knows M.

4. Final Remarks

In this work, we have presented a new epistemic logic to reasoning about security protocols. This logic introduces a new semantics based on structured propositions. Instead of building formulas from atomic propositions, they are built from expressions. The latter, are any peace of information that can appear in protocols: keys, messages, agents, encrypted messages or any combination of these informations in pairs.

We propose this new semantics and an axiomatization for this logic. We also prove soundness and completeness.

Acknowledgements: We would like to thank anonymous referees for their profitable comments.

References

Boureanu, I., Cohen, M., and Lomuscio, A. (2009). Automatic verification of temporal-epistemic properties of cryptographic protocols. *Journal of Applied Non-Classical Logics*, 19(4):463–487.

Cohen, M. and Dam, M. (2007). A complete axiomatization of knowledge and cryptography. In *22nd IEEE Symposium on Logic in Computer Science (LICS 2007), 10-12 July 2007, Wroclaw, Poland, Proceedings*, pages 77–88.

Dolev, D. and Yao, A. C. (1983). On the security of public key protocols. *Information Theory, IEEE Transactions on*, 29(2):198–208.

Fagin, R., Halpern, J. Y., Moses, Y., and Vardi, M. Y. (1995). *Reasoning About Knowledge*. MIT Press, Cambridge, Massachusetts.

Kramer, S. (2008). Cryptographic Protocol Logic: Satisfaction for (timed) Dolev-Yao cryptography. *Journal of Logic and Algebraic Programming*, 77(1–2).

Lamport, L. (1978). Time, clocks, and the ordering of events in a distributed system. *Commun. ACM*, 21(7):558–565.