UNIVERSITÀ DEGLI STUDI DI PALERMO
DOTTORATO DI RICERCA

Distributed Misbehaviour Detection in sistemi multi-robot cooperanti

Federico Massa

21 Agosto 2017

1 INTRODUZIONE

La maggiore disponibilità di risorse computazionali degli ultimi decenni ha causato un crescente interesse verso algoritmi distribuiti in applicazioni robotiche [1]. In particolare nell'ambito del Controllo, il cambio di paradigma in questo senso ha reso possibile la cooperazione tra agenti eterogenei, ognuno con diversi tipi di sensori di bordo, potenza computazionale e attuativa, che, eventualmente avvalendosi di sistemi di comunicazione per lo scambio di informazioni, sono in grado di eseguire insieme un compito assegnato, incrementando l'efficienza con cui viene svolto [2].

Lo sviluppo di tali algoritmi consente dunque di aprire la strada a "società" di robot [3], indipendenti e consapevoli della presenza di altri agenti, che possono comunicare tra loro scambiandosi informazioni sull'ambiente. Ognuno di essi deve rispettare alcune regole imposte dalla sua appartenenza a tale gruppo, che ne garantiscono il corretto funzionamento nel pieno rispetto dei vincoli imposti dall'ambiente (un tipico esempio di riguarda la sicurezza necessaria laddove sia prevista l'interazione con esseri umani) e dal compito assegnato. Come nelle società umane, la cooperazione può svolgere un ruolo determinante, ed esistono già esempi di questo tipo nel campo della robotica. Si pensi ad esempio ad un contesto di tipo autostradale in cui più veicoli (autonomi o semi-autonomi) si mantengono in formazione di *platoon* (Fig. 1), e si coordinano tramite lo scambio di informazioni sensoriali tra vicini [4], al fine di raggiungere in maniera più efficiente la destinazione.

In questo progetto ci interessiamo a due possibili cause che possono generare deviazioni (*misbehaviours*) dal comportamento corretto dei robot: la presenza di quelli che da ora in poi definiremo *agenti non cooperanti*, ovvero che non seguono (in modo anche parziale) le regole sociali, e i cyber-attacchi che consistono nella comunicazione (da parte di un agente corrotto), di informazioni scorrette sullo stato del sistema.

In questa ipotesi, diventa dunque importante realizzare dei sistemi di verifica del comportamento degli agenti. In entrambe le situazioni indesiderate descritte, il processo di rilevamento e della possibile identificazione dell'agente compromesso può difficilmente essere portato a compimento da un singolo agente, a causa del fatto che ognuno può possedere una conoscenza solo parziale dello stato degli altri. Lo scambio tra gli agenti delle informazioni possedute sull'ambiente circostante può rendere questo problema meglio affrontabile, ma introduce anche un problema di sicurezza, rendendo possibile che un agente malevolo interferisca durante la comunicazione.

L'obiettivo principale di questo progetto è lo sviluppo di un framework distribuito per la rivelazione di misbehaviours e di una classe di cyber-attacchi in società multi-robot eterogenee e cooperanti.

Figura 1: Esempio di società cooperante: veicoli in formazione di platoon.

2 STATO DELL'ARTE

Il problema della *misbehaviour detection* non è stato ancora molto affrontato in robotica, mentre si incontra spesso in informatica sotto il nome di *intrusion detection* (ID), dove lo scopo è quello di individuare eventuali attacchi malevoli a danno di uno o più nodi della rete [5][6]. L'architettura di molti algoritmi con questo obiettivo è centralizzata: la raccolta dei dati avviene sui singoli nodi, ma l'analisi viene condotta su un solo nodo o su un numero ristretto. Sebbene le applicazioni robotiche presentino delle sostanziali differenze rispetto alle reti informatiche, molti dei concetti sono analoghi, ed è pertanto importante confrontarsi con gli studi di questo tipo. Uno dei problemi comuni dati dalla centralizzazione è il

cosiddetto *single point of failure*, ovvero il fatto che la riuscita di un attacco da parte di un software/agente malevolo sul nodo centrale possa compromettere la sicurezza dell'intero sistema. Un altro problema di questo tipo di sistemi è la *scalabilità*, in particolare in quegli ambienti in cui il numero di agenti non sia determinabile a priori e può variare nel tempo.

Più raramente il tipo di architettura scelta per questi sistemi è *distribuita* [7]. In particolare in contesti robotici, questa risulta essere molto flessibile, e particolarmente adatta per ambienti eterogenei e in cui la *riconfigurabilità* sia una qualità importante [3]. Alcuni studi riguardano lo sviluppo di un sistema di verifica locale basato sullo studio del moto [8], ma assumono di conoscere il modello dinamico degli agenti, ipotesi che ai fini di questo progetto è limitante. Per quanto riguarda gli attacchi è stata già studiata la possibilità di riconoscere un agente che invia informazioni scorrette grazie alla comunicazione con gli altri e il raggiungimento di un consenso[9].

3 OBIETTIVI DEL PROGETTO

Il lavoro che viene proposto riguarda lo sviluppo di un framework per la realizzazione di un Misbehaviour Detection System (MDS) in ambienti robotici eterogenei e cooperanti, con l'obiettivo di rendere il più possibile semplice la riconfigurazione del sistema. Come già accennato, i tipi di comportamento scorretto che vogliamo identificare sono due:

- *Agente non cooperante*: un agente che non rispetta le regole della società (potrebbe idealmente far parte di una società diversa o essere malfunzionante) [3];
- *Deceptive attacker*: un agente malevolo o malfunzionante che comunica informazioni errate agli altri agenti [6].

Immaginando che il MDS sia installato su uno o più agenti della "società" (gli *osservatori*), e che abbia a disposizione informazioni sensoriali adeguate per svolgere tale compito, il progetto si articola nei passi seguenti:

Studio dell'ambiente Durante questa fase preliminare, il MDS studia l'ambiente circostante, accumulando tutti i dati necessari per svolgere correttamente il suo compito. L'elaborazione di mappe dell'ambiente è un problema molto studiato in robotica [10].

Riconoscimento del comportamento Il MDS costruisce ora, partendo da dati sensoriali di basso livello raccolti in un certo intervallo di tempo, la propria conoscenza del comportamento degli agenti combinando informazioni a formare una conoscenza sempre di più alto livello di astrazione. Estendendo questo processo nel tempo sarà possibile riconoscere una sequenza di azioni intraprese dagli agenti osservati. Per la realizzazione dell'algoritmo verranno valutati approcci deterministici e di machine learning, e si cercherà di darne una validazione formale.

Verifica delle regole Una volta individuate le sequenze di azioni degli agenti osservati ed avendo codificato il sistema di regole a priori, è possibile verificare che la sequenza riconosciuta rispetti le regole o meno. In Fig.2 ne è mostrato un esempio.

Consenso A causa della parziale conoscenza degli agenti osservati dovuta a limiti di portata o accuratezza dei sensori, ostacoli che impediscono la visione in una certa area e altri, non è sempre possibile il riconoscimento di una particolare azione, quantomeno in maniera efficiente. Lo scambio di informazioni tra robot e il raggiungimento di un consenso sul comportamento possono risolvere il problema [11]. Questo, in realtà, introduce il problema dell'affidabilità delle informazioni ricevute dagli altri agenti.

Attribuzione di una reputazione Per mitigare i danni inferti da un attaccante *deceptive*, il riconoscimento del comportamento e la verifica delle regole vengono effettuati dapprima con le sole informazioni possedute dall'osservatore. Solo successivamente si utilizzano le informazioni possedute dagli altri, le quali vengono valutate e confrontate. Nel caso in cui vi sia una contraddizione tra queste informazioni, un possibile attacco viene rilevato. Studiare come individuare l'attaccante è uno degli obiettivi del progetto. Dalla verifica delle regole e l'eventuale consenso, invece, è possibile rilevare gli agenti non cooperanti. Un obiettivo del progetto è anche quello di sviluppare un sistema di reputazione per gli agenti, in modo che ad ogni azione riconosciuta venga attribuito un punteggio basato sulla correttezza o meno della sua esecuzione. Dopo un tempo sufficiente sarà stato creato un profilo dell'agente che ne descrive le caratteristiche comportamentali fondamentali, a disposizione di tutti gli agenti della società affinché possano comportarsi di conseguenza al momento dell'interazione.

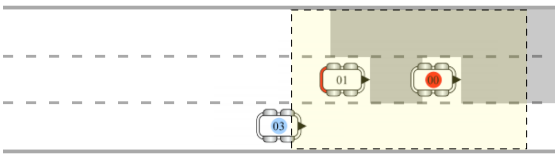

Figura 2: Autostrada in cui vige la regola del tenere la corsia più a destra possibile. Un agente non cooperante (00) viene osservato da un altro (03), che avendo piena visibilità sulla prima corsia riconosce un comportamento non conforme alle regole sociali.

4 TIMELINE DEL PROGETTO

Il progetto potrà attuarsi nella seguente maniera:

1° anno - Progettazione

1. Definizione del problema e studio delle ricerche già esistenti
2. Individuazione di contesti applicativi adeguati in cui studiare il problema
3. Sviluppo framework di simulazione
4. Sviluppo algoritmi di riconoscimento dei comportamenti

2° anno - Test

1. Studio/sviluppo di metodi di codifica delle regole sociali
2. Implementazione e test degli algoritmi all'interno del framework di simulazione nei diversi contesti applicativi

3° anno - Sperimentazione

1. Individuazione modalità di sperimentazione adeguata, ottimizzando il rapporto tra i costi e l'efficacia con cui l'esperimento dimostra la generalità della soluzione trovata
2. Progettazione dell'esperimento (soluzioni hardware adeguate, complessità dell'ambiente necessaria per ottenere realismo, ricerca sito dell'esperimento)
3. Installazione del MDS sul robot fisico e test.

RIFERIMENTI BIBLIOGRAFICI

[1] N. A. Lynch, *Distributed Algorithms*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 1996.

[2] D. Vail and M. Veloso, "Dynamic multi-robot coordination," in *In Multi-Robot Systems: From Swarms to Intelligent Automata, Volume II*. Kluwer Academic Publishers, 2003, pp. 87–100.

[3] A. Bicchi, A. Fagiolini, and L. Pallottino, "Towards a society of robots: Behaviors, misbehaviors, and security," *IEEE Robotics and Automation Magazine*, 2010.

[4] L. Y. Wang, A. Syed, G. G. Yin, A. Pandya, and H. Zhang, "Control of vehicle platoons for highway safety and efficient utility: Consensus with communications and vehicle dynamics," *Journal of Systems Science and Complexity*, vol. 27, no. 4, pp. 605–631, Aug 2014.

[5] J. Saranya and G. Padmavathi, "A brief study on different intrusions and machine learning-based anomaly detection methods in wireless sensor networks," *International Journal of Advanced Networking Applications*, vol. 6, no. 4, pp. 2414 – 2421, 2015.

[6] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Automat. Contr*, 2013.

[7] A. P. Grzech, "Optimal monitoring system for a distributed intrusion detection system," in *14th International Symposium on Artificial Life and Robotics*, Oita, Japan, 2009.

[8] A. Fagiolini, G. Valenti, L. Pallottino, G. Dini, and A. Bicchi, "Decentralized intrusion detection for secure cooperative multi-agent systems," *46th IEEE Conference on Decision and Control*, 2007.

[9] A. Bicchi, A. Fagiolini, G. Dini, and I. M. Salvino, "Tolerating, malicious monitors in detecting misbehaving robots," *IEEE International Workshop on Safety, Security and Rescue Robotics*, 2008.

[10] S. Thrun, "Robotic mapping: A survey," in *Exploring Artificial Intelligence in the New Millenium*, G. Lakemeyer and B. Nebel, Eds. Morgan Kaufmann, 2002.

[11] R. Olfati-Saber, J. Alex Fax, and R. Murray, "Consensus and cooperation in networked multi-agent systems," vol. 95, pp. 215–233, 01 2007.