UNIVERSITÀ DEGLI STUDI DI PALERMO
DOTTORATO DI RICERCA

Distributed Mesbehaviour 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 prendere decisioni indipendenti. Lo sviluppo di tali algoritmi consente dunque di aprire la strada a "società" di robot[2], consapevoli della presenza di altri agenti, con cui eventualmente possono cooperare per svolgere dei compiti e scambiare informazioni. In generale la capacità di inferenza richiesta per ognuno degli agenti dipende molto dal tipo di ambiente in cui essi devono lavorare e dai vincoli che devono rispettare. Tuttavia, ogni agente deve rispettare alcune regole imposte dalla sua appartenenza a tale "società", che ne garantiscono il corretto funzionamento nel pieno rispetto dei vincoli imposti dall'ambiente (un tipico esempio di vincolo riguarda la sicurezza necessaria in un ambiente in cui possono esserci umani o elementi fragili) e dal compito assegnato. La corretta dinamica di una società di questo tipo può essere compromessa dalla presenza di un "intruso", ovvero un agente che non rispetta (in modo anche parziale) le regole. Si noti che non è necessario che il comportamento di tale intruso sia compatibile con un malfunzionamento, ma è sufficiente che esso non rispetti le regole della società alla quale dovrebbe appartenere. L'identificazione di tale intruso può in certi casi essere effettuata singolarmente dagli agenti, ma tipicamente questo non è possibile, a causa del fatto che ogni agente "osservatore" possiede una conoscenza solo parziale dello stato degli altri. La comunicazione tra

gli agenti delle informazioni possedute da ciascuno sull'ambiente circostante può rendere possibile questo obbiettivo, ma pone importanti problemi di sicurezza, rendendo possibile che un agente malevolo introduca informazioni corrotte che possono essere propagate nel sistema. Gran parte del lavoro su queste tematiche studia approcci centralizzati o ibridi, che tipicamente presentano problemi di scalabilità. In questo progetto si propone lo studio di algoritmi completamente distribuiti per la risoluzione del problema della *intrusion detection* in contesti robotici.

2 STATO DELL'ARTE

Il problema della *intrusion detection* (ID) viene tipicamente studiato in reti di computer in cui si vuole cercare di individuare eventuali attacchi malevoli a danno di uno o più nodi della rete (si veda, ad esempio). L'approccio di molti software che offrono questo servizio è centralizzato (es. Tripwire): il raccoglimento 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 e alcune tecniche possono essere riutilizzate, 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 è determinabile a priori e può variare nel tempo. Questi problemi sono mitigati in architetture ibride, dette *gerarchiche*[3], in cui diversi nodi applicano localmente un algoritmo di ID, mentre la decisione finale viene eseguita da un nodo centrale che sfrutta le preanalisi condotte localmente. Più raramente il tipo di architettura scelta per questi sistemi è di tipo *distribuito*, che per sua natura risulta molto flessibile. In particolare in contesti robotici, tali architetture sono molto adatte ad ambienti *eterogenei*, in cui ogni agente ha diverse capacità attuative e cognitive, e *riconfigurabili*[2], dato che non necessitano di un'infrastruttura centralizzata. Esistono molti studi che sfruttano architetture distribuite per la realizzazione di compiti coordinati tra più robot (es. [4]), ma il problema della ID in questo ambito è poco studiato. Si pensi, ad esempio, ad un contesto di tipo autostradale in cui più veicoli (autonomi o semi-autonomi) stanno in formazione di *platoon*, e si coordinano tramite lo scambio di informazioni sensoriali tra vicini[5]. In questo esempio, i veicoli si muovono insieme per realizzare lo stesso compito (raggiungere una determinata destinazione), in un modo più efficiente di quanto farebbero senza coordinamento (risparmiando carburante, per esempio). Un ipotetico attaccante potrebbe immettere nel sistema informazioni corrotte per rompere la formazione, ad esempio provocando oscillazioni forzate. È importante, quindi, riconoscere che è in atto un attacco e comportarsi di conseguenza.

3 OBIETTIVI DEL PROGETTO

Il lavoro che viene proposto riguarda lo sviluppo di un framework per la realizzazione di un Intrusion Detection System (IDS) in ambienti robotici eterogenei (ed eventualmente coo-

peranti), con l'obiettivo di rendere il più possibile semplice la riconfigurazione del sistema. Occorre prima di tutto definire cosa si intende in questo caso per *intruso*. In una società multi-robot, esso può essere:

- un agente che non rispetta le regole della società (potrebbe idealmente far parte di una società diversa);(society)
- un agente malevolo o malfunzionante che diffonde informazioni errate nel sistema. (articoli)

Immaginando che l'IDS sia installato su uno o più agenti della "società", e che abbia a disposizione informazioni sensoriali adeguate per svolgere tale compito, l'obiettivo del progetto è quello di replicare i seguenti passi:

Studio dell'ambiente Durante questa fase preliminare, l'IDS studia l'ambiente circostante, accumulando tutti i dati necessari per svolgere correttamente il suo compito. L'elaborazione di mappe .....

Riconoscimento del comportamento L'IDS costruisce ora, partendo da dati sensoriali di basso livello su un certo intervallo di tempo, la propria conoscenza del comportamento degli agenti combinando informazioni sempre di più alto livello. Estendendo questo processo nel tempo sarà possibile riconoscere una sequenza di azioni intraprese dagli agenti osservati. I principali studi su ques

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

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. 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 che cerca di diffondere informazioni sbagliate nel sistema, 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 osservatori, le quali vengono valutate e confrontate con quelle provienienti da tutti gli altri. Nel caso in cui vi sia una contraddizione tra queste informazioni, un possibile attacco viene rilevato. Dalla verifica delle regole e l'eventuale consenso, invece, è possibile rilevare quegli agenti che non rispettano le regole della società. In quegli ambienti in cui abbia senso farlo, si può tenere conto del comportamento di un agente nel tempo attribuendo un punteggio alle sue azioni, positivo quando si comporta secondo le regole e negativo quando non lo fa. Inoltre, avendo riconosciuto e giudicato il suo comportamento, è possibile costruire un profilo dell'agente, che ne individui le

caratteristiche di comportamento fondamentali. Questo può essere particolarmente utile in grandi società, come potrebbe essere quella formata da tanti veicoli autonomi che viaggiano in autostrada, perché in questo modo due veicoli che si incontrino per la prima volta potrebbero già avere informazioni l'uno sull'altro e plasmare il loro comportamento su questo.

Fabio Pasqualetti - www.fabiopas.it
[6], [7], [8]

RIFERIMENTI BIBLIOGRAFICI

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

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

[3] M. S. I. Mamun and A. F. M. S. Kabir, "Hierarchical design based intrusion detection system for wireless ad hoc sensor network," *International Journal of Network Security & Its Applications*, vol. 2, no. 3, pp. 102 – 117, 2010.

[4] 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.

[5] 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.

[6] M. Toulouse, B. Q. Minh, and P. Curtis, "A consensus based network intrusion detection system," in *The 5th International Conference on IT Convergence and Security*, Kuala Lumpur, Malaysia, 2015.

[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] 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.