Poster Abstract: Security and Advanced Control Issues in a Robotic Platform for Monitoring and Relief

Antonio Danesi
Centro Interdipartimentale di Ricerca "E. Piaggio"
Università di Pisa
Pisa, Italy
antonio.danesi@ing.unipi.it

Ida M. Savino
Dipartimento di Ingegneria dell'Informazione
Università di Pisa
Pisa, Italy
ida.savino@iet.unipi.it

Riccardo Schiavi
Centro Interdipartimentale di Ricerca "E. Piaggio"
Università di Pisa
Pisa, Italy
riccardo.schiavi@ing.unipi.it

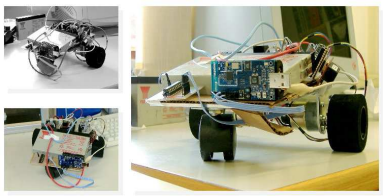

Figure 1: RAiN agent prototype layout.

ABSTRACT

This paper provides an architectural overview and a first implementation of an heterogeneous agent network composed by mobile robots of different scale and purposes able to establish a secure group connection among them and with the fixed infrastructure. A road tunnel patrolling and first relief application has been issued.

1. INTRODUCTION

This poster will provide an overview of the architecture we are developing according to the *Tunnel Disaster Scenario* studied in the context of EU-funded RUNES project (http://www.ist-runes.org). The architecture consists of autonomous mobile robots moving along a road tunnel for cars and trucks, collecting data and reacting to emergencies in order to provide first relief services to people and goods. The robotic platform is supported by a fixed tunnel infrastructure that provides cameras and video elaboration along the tunnel, collects data from robots and coordinate actions. Two kinds of robots move and survey the environment: *GaIN* (Gateway Infrastructure Network) agents are camera-equipped mid-size mobile robots and *RAiN*(Robotic Aided Networking) agents are small size inexpensive mobile systems with low-cost sensors as (fig.1). These agents form with the tunnel infrastructure an heterogeneous mobile sensor and actuator network. Control issues in this architecture involve the study of distributed algorithms to efficiently cover the road tunnel during patrolling, obstacle avoidance and wireless network coverage maintenance via mobile agents. We made particular efforts to realize RAiN platforms as the cheap sensor/actuator nodes. The core of the architecture of the small agent comes from integrating the Tmote Sky sensor node with a PSoC microcontroller to control drivers and collect odometry data of the small vehicle. A crucial issue for mobile robots is absolute localization, in our work we adopt vision as main technology. RAiN agents don't have sensors to identify absolute position. Road tunnel fixed cameras can identify agents by visual marks placed on their chassis and calculate their absolute positions. On the other hand, GaIN agents can localize themselves by means of tunnel graphic marks. Furtermore, theyhave responsable for localizing RAiN when they appen to be in areas not covered by fixed cameras.
The RAiN and GaIN agents cooperate toward the distributed control task according to the *group communication* model. In this model, a mobile agent becomes a new member of the group by explicitly joining it (i.e., at tunnel entrance). As a member of the group, the agent may broadcast messages to the other members. Later on, the agent may voluntarily leave the group, or, if compromised, may be forced to. After that event, the agent cannot send messages to, or receive messages from, the group. From a security perspective, the agents form a wireless network that is vulnerable to serious attacks. Actually, it must be avoided that adversaries, equipped with a simple radio receiver/transmitter, easily eavesdrop conversations or inject/modify packets thus compromising the agent network.

2. ARCHITECTURE

We simulate the road tunnel environment with our lab equipment. A fixed camera connected to a PC performs as the fixed infrastructure of the tunnel, capable to store data, elaborate orders to mobile platforms and furnish localization services. The GaIN agents are built over commercial mobile robots, *Koala*, equipped whit a laptop pc and camera. These agents have enough computational capabilities to implement algorithms to navigate known and unknown environments while building and updating maps. RAiN agents are built on a 802.15 wireless sensor network node, communicating with a microcontroller that drives two actuators to move the agent. They can extend their communication ranges simply moving. In case of detaching of portions of tunnel, these agents can be used to reestablish connectivity.

3. HARDWARE INTEGRATION

GaIN agents have a classical solution of Pentium boards that control middle size robotic platforms and elaborate camera sensor data. Layout of RAiN agents have been designed for functionality despite extreme low cost. Tmote Sky boards already implement 802.15 protocol and the board has programmable CPU and sensors. PSoC microcontrollers have versatility and programming tools. The board we implemented ties these CPU's over RS232 link. PSoC drives two

motors able to move RAiN agent as an unicycle with speed or position reference. Tmote Sky can make the agent to follow a desired path programming the PSoC to implement a proper control on motors.

4. VISUAL LOCALIZATION AND COLLISION AVOIDANCE

GaIN agents patrol environment using our Visual SLAM for Servoing (VSLAMS) algorithm that perform localization and map building with visual servoing techniques [1]. This makes GaIN agents able to dynamically update maps with changes and perform safe path planning in known environment. Infrastructure and GaIN agents perform visual recognition of marks over chassis of agents. Techniques involved in video processing are SIFT (Scale Invariant Feature Transform) decompositions [4], contour analysis and homographic projections. Each RAiN agent can ask for a localization service to the infrastructure and to GaIN agents, sharing the visual informations able to identify univocally one vehicle. In order to avoid collisions among the RAiN agents a decentralized cooperative algorithm has been studied in our lab [5] and implemented dealing with limitations in hardware computation capabilities. Secure connections on localization services are necessary not to be subject to tampering action.

5. SECURITY

In order to protect group communication, RAiN and GaIN agents share a symmetric *group-key*. Techniques based on public key cryptography, e.g., digital signatures, that are usually used to achieve broadcast authentication in traditional wired networks, cannot be used. Hence, the agents use the group-key to encrypt messages broadcast within the group so that anyone that is not part of the group can neither access nor inject/modify messages. This solution is complicated by the fact that the group membership may change. New agents can *join* the group after the deployment of the application, whereas an agent *leaves* the group when it has terminated its mission. Besides, agents are particularly exposed to the risk of being compromised and thus it may be necessary to force them to leave the group. When a new agent joins the group, that agent must not be able to decipher previous messages encrypted with an old key even though it has recorded them (*backward security*). When an agent leaves, or is forced to leave, the group, the agent must be prevented from accessing the group communication (*forward security*). In this model, forward and backward security are provided via rekeying. When a member joins or leaves the group, a new group-key must be distributed in order to guarantee both backward and forward security. In large and/or dynamic groups, this *reactive* approach to group-key management may incur in high rekeying overhead. Nevertheless, the approach has the advantage that a new node can immediately join the group and a compromised member can be promptly forced to leave as soon as it is discovered. Due to the severe resource limitations of agents, the rekeying protocol must aim at a trade-off between security and resource consumption. For these reason we adopt a secure and scalable rekeying protocol that levers on two basic mechanisms [2]: key-chains, a lightweight authentication mechanism based on the Lamport's one-time passwords [3], and a Logical Key Hierarchy (LKH), a technique for secure and scalable group rekeying [6]. In brief, LKH allows us to reduce the communication overhead by reducing the number of rekeying messages. Upon receiving new keys without additional overhead (i.e., signature), every agent is able to immediately verify its authenticity by means of hash functions.

6. CONCLUSIONS

In this poster we provided an overview of a secure and advanced robotic architecture. We have shown an implementation of robotic sensor network, where heterogeneous mobile robots patrol using visual feedback and secure group communication.

7. ACKNOWLEDGMENTS

The work of undergraduate students Alessandro Convalle, Lorenzo Decaria, Isidoro S. La Porta is gladly acknowledged.

8. ADDITIONAL AUTHORS

Additional authors: Antonio Bicchi (Centro Interdipartimentale di Ricerca "E. Piaggio", Università di Pisa, email: `bicchi@ing.unipi.it`) and Gianluca Dini (Dipartimento di Ingegneria dell'Informazione, Università di Pisa, email: `gianluca.dini@unipi.it`).

9. REFERENCES

[1] A. Danesi, D. Fontanelli, and A. Bicchi. Towards cooperative visual-based localization, mapping, and servoing. 2004. Proc. IEEE Mediterranean Conf.

[2] G. Dini and I. Savino. Scalable and secure group rekeying in wireless sensor networks. *Prooc. IASTED PDCN*, February 2006.

[3] L. Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, November 1981.

[4] D. G. Lowe. Object recognition from local scale-invariant features. *International Conference on Computer Vision*, pages pp. 1150–1157, September 1999.

[5] L. Pallottino, V. G. Scordio, E. Frazzoli, and A. Bicchi. Decentralized cooperative conflict resolution for multiple nonholonomic vehicles. In *Proc. AIAA COnf. on Guidance, Navigation and Control*, page (in press), 2005.

[6] C. K. Wong, M. G. Gouda, and S. S. Lam. Secure group communications using key graphs. *IEEE/ACM Transactions on Networking*, 8(1):16–30, February 2000.