Distributed Access Control for Decentralized Information Sharing

Zia Hayat, Jeff Reeve, Chris Boutle, Martin Field, and Peter Tuson

***Abstract*— The research described in this paper was carried out as part of the Systems Engineering for Autonomous Systems (SEAS) Defense Technology Centre (DTC), which is a UK MoD initiative looking into future unmanned technology. The main objective of this study was to assess novel access control mechanisms, which may enable increasingly autonomous agent applications operating in ubiquitous computing and communications networks. Ubiquitous networks provide opportunities for a distributed and ad-hoc command and control (C2) and information sharing environment, but challenge traditional information security techniques, which must be adapted to ensure the best exploitation of the prospect. In particular machines must be able to authenticate and prove authorization to securely access distributed services, in an agile and robust manner. Currently many ad-hoc computing applications use simple privilege mechanisms or human intuition to control access to potentially sensitive services, such as reconnaissance information. However such mechanisms lead to a rigid and centralized information sharing model which does not scale well, especially when considering future distributed computing capabilities in which machines need to autonomously provide and consume information based services. Results from testing carried out into the perceived operational benefits of alternative (current centralized and future distributed) access control models for a Mobile Ad-hoc Network (MANET) are discussed. In the MANET individual nodes (or agents) represent mobile devices needing to share information in a decentralized and ad-hoc manner. A candidate architecture for realizing a distributed access control mechanism incorporating context is then defined.**

***Index Terms*— Access Control, Decentralized Information Sharing, Security and Ubiquitous Computing**

I. Introduction

COMPUTING and communications networks are impacting all aspects of our lives, where almost every physical activity can be electronically logged and analyzed in real-time. This has been facilitated by mobile computing devices such as personal digital assistants (PDAs) and laptop computers, which are capable of communicating through heterogeneous interfaces (WiFi, Bluetooth etc.). Such devices can be used to collect, store and transmit vast amounts of potentially sensitive data in an always-on manner. This is evident in projects such as Systems Engineering for Autonomous Systems (SEAS) Defense Technology Center (DTC) [1], Autonomous Learning Agents for Decentralized Data and Information Networks (ALADDIN) [2] and related work on decision making with multi-agent systems (MAS) in wireless sensor networks [3], [4], where autonomous learning agents[1] need to share information in a distributed and ad-hoc manner to efficiently achieve time-sensitive objectives. For example imagery sensor agents may be used to monitor and stream reconnaissance for law enforcement purposes. In such scenarios agents need to provide and consume sensitive information services in real-time, therefore it is imperative that information exchange is timely as well as secure.

So far autonomy has been defined and studied using two distinctive approaches in the autonomous agent's research community. Firstly it has been characterized as the degree of self-control an agent has over its own decisions, which is assigned by a higher-level authority, e.g. a supervisor (human or machine), this was introduced in [5] as decision autonomy. Decision autonomy is a satisfactory concept when considering agents in closed environments. However as the operational environment becomes more uncertain (real-life) then an additional understanding of autonomy with respect to self-capability is required as described in [6]; this was introduced in [5] as self-capability autonomy. This latter approach is an assessment of an agent's ability, to accomplish its assigned mission objectives with minimal external co-operative intervention.

The quest for increasing self-capability autonomy can be seen in the field of autonomic computing where research [7], [8]–[10] is focusing on capabilities which can more effectively manage the complexities associated with the ubiquitous nature of modern networks. According to [11] the aim of autonomic computing is to increase the sophistication of individual components and networks, so that they can become "self-managing" and take corrective actions in accordance with overall system-management objectives. This is analogous to the human nervous system which controls bodily functions such as heart rate, breathing and blood pressure without any

The work reported in this paper was funded by the Systems Engineering for Autonomous Systems (SEAS) Defense Technology Centre (project IF024) established by the UK Ministry of Defense.

Zia Hayat and Jeff Reeve are with the Communications Laboratory, School of Electronics & Computer Science, Faculty of Engineering, University of Southampton, Southampton, Hampshire SO17 1BJ, UK (phone: +44 (0)1276 603681; fax: +44 (0)1276 603112; e-mail: zia.hayat@baesystems.com).

Chris Boutle, Martin Field and Peter Tuson are with BAE Systems, Frimley, Camberley, Surrey GU16 7EX, UK.

conscious attention on our part.

The need for increasingly self-capable systems is partly driven by the cost of human labor, for example the expenditure on managing networks currently exceeds equipment costs by a ratio of up to 18:1 [12]. As well as excessive costs manual control by human operators results in overly complex and inefficient processes. From a security perspective such complexity can lead to inadequate protection as well as inhibiting business requirements. This is evident in current electronic access control procedures which provide a coarse level of granularity, and are therefore reliant upon human intervention to securely enable the required level of access to services.

The mobile and plug-and-play nature of modern computing devices is facilitating distributed computing. One such technology is the Mobile Ad-hoc Network (MANET) which enables groups of agents to form ad-hoc coalitions capable of sharing information in a distributed manner. The operational benefits of MANETs are:

- *Fault-tolerance* – No single point of data processing or communications failure.
- *Scalability* – Not subject to communication or computational bottlenecks.
- *Flexibility* – Support on-line addition or deletion of nodes (i.e. plug-and-play).

It is envisaged that MANETs will be used to enable a wide range of applications, from search and rescue operations in the emergency services to the improvement of business processes in a corporate environment. In such scenarios the agents which make up a MANET need to constantly share sensitive information-based services [3,4]. Therefore it is essential to control access to such services to preserve the security principle of least privileges and prevent information overload.

This paper builds on previous work described in [5] by providing a quantitive assessment of alternative access control mechanisms for MANETs. Section II illustrates the need for alternatives to current centralized access control mechanisms. The scenario and simulation used to undertake a cost-benefit analysis of using a decentralized as opposed to a centralized access control model is defined in section III, with results and analysis given in section IV. Section V describes a candidate role-based context-dependent access control model which could enable secure decentralized information sharing. Conclusions and suggestions for future work are then given in section VI.

II. Centralized Access Control for MANETs?

Access control is based upon the subject-privilege-object methodology, where a subject (agent) has an associated privilege (read, write etc.) with respect to some object (information service). In the majority of current ad-hoc computing applications which adhere to the subject-privilege-object methodology, numerous factors including a subjects identity are manually considered for authorization purposes by a central 'security-aware' authority (i.e. humans). For example in many Home Land Security (HLS) systems drone agents such as SkySeer [13] are used to carry out surveillance operations, all interactions with such drones are executed via a central control station. For security purposes the control station is used as a human in the loop mechanism to manage the flow of all information to/from drone agents due to its potentially sensitive nature. However this limits the possibility of forming a MANET based coalition between drone agents and other 'intelligent' agent types such as human patrol guards, where agents could directly interact in a Peer-to-Peer (P2P) network, sharing information services in real-time. Such P2P coalitions require individual agents to locally (decentralized) enforce authentication and authorization decisions.

The alternative information exchange architectures due to centralized and decentralized access control are illustrated in fig.'s 1 and 2 respectively. Due to the largely remote-controlled operating mode of current agent technologies such as an Unmanned Air Vehicle (UAV), their information exchange requirements are limited to a centralized model between the agent and its current control station as depicted in fig. 1. In fig. 1 the agents can be seen to have static and continuous communications with a control station. Such communications may be for telemetry, Command and Control (C2) and sensor feed purposes. However as agents become more self-capable their communications are likely to become less constrained, giving rise to more complex distributed interactions and therefore a swarm MANET.

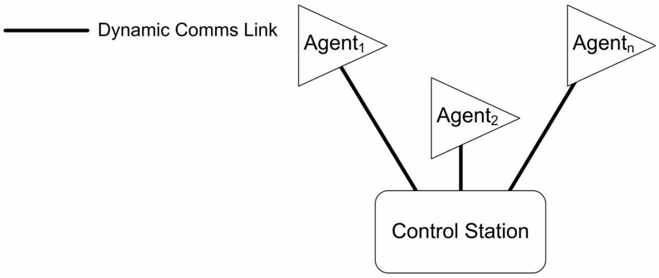


Fig. 1. Current MANET Information Exchange Architecture.

A swarm-like MANET setup is illustrated in fig. 2, where the information exchange requirements between agents and a control station are much more ephemeral. In this arrangement the individual agents will be capable of communicating amongst themselves enabling increasingly sophisticated Machine-to-Machine (M2M) interactions.

A key requirement of surveillance MANETs is Decentralized Data Fusion (DDF), where sensor agents need to correlate observations by sharing information in a distributed and ad-hoc fashion. Using centralized access control such sensor agents would have to fuse data through an authorized central agent(s), to ensure that only relevant data from those agents with common areas of observation is fused. In this situation the central authority can either fuse the data itself or pass on relevant information to individual sensors for

[1] An agent may be human or machine.

subsequent fusion. However it is hypothesized that a centralized access control model will undermine the potential benefits (described in section 1) of a distributed computing functionality by introducing unacceptable:

- Latencies – due to bottlenecks in information sharing.
- Levels of risk – due to a single point of failure.

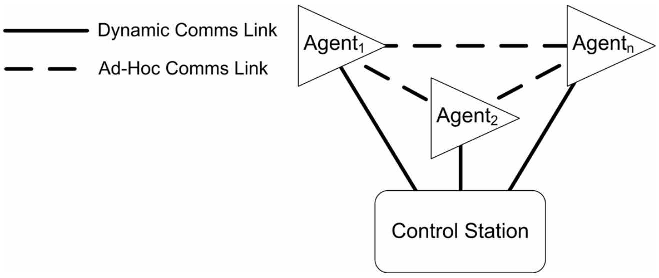


Fig. 2. Envisaged MANET Information Exchange Architecture.

A simple sensor network is illustrated in fig. 3 where three image sensors (S_1, S_2 and S_3) are observing an area of interest. Due to their locations S_1 and S_2 have an intersecting observation area ($A_{1\text{-}2}$) and therefore need to share information as do S_2 and S_3 for the area $A_{2\text{-}3}$.

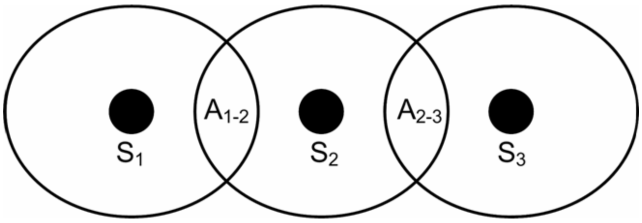


Fig. 3. Sensors need to share information in a distributed and ad-hoc fashion.

III. Scenario and Simulation

A. Overview

In order to assess the relative merits of centralized and decentralized access control mechanisms a cost-benefits analysis has been undertaken through simulation. The simulation involves a MANET of multiple ground and air based autonomous agents in a HLS mission, as illustrated in fig. 4. The objective of the mission is to carry out surveillance and tracking of target agents for their capture. For simplicity, surveillance and tracking activities are performed by air sensor agents and capture activities by ground effector agents. Therefore sensor agents (S_1 to S_3) need to share information to correlate observations on the target (T_1) and provide timely information to authorized effector agent(s) (E_1) regarding the location of a target(s). To represent the movement of sensors and capturers as well as tasking by mission managers simple probabilistic decision-making models based upon previous modeling in [14] are used. In the simulation a centralized access control model is represented by a centralized information exchange architecture, and similarly a decentralized access control model is represented by a decentralized information exchange architecture.

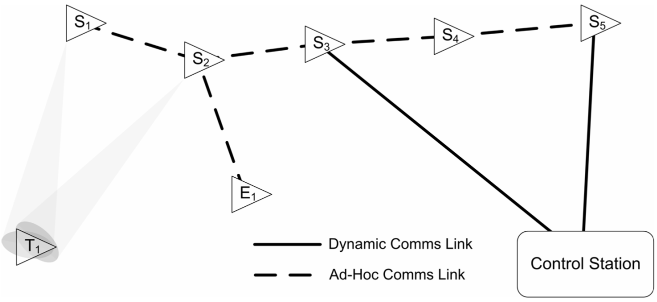


Fig. 4. A decentralized information exchange architecture introduces security challenges.

The scenario has been implemented in Requirements Driven Development (RDD)-100 and utilizes generic models developed previously by BAE Systems. RDD-100 is an object-oriented systems engineering tool which enables requirements definition, simulation and analysis of engineering problems. In the model all air-based surveillance and tracking agents are represented as sensors, similarly ground-based capture agents are represented as effectors with target agents modeled as targets. For the purposes of this exercise traditional control station or mission managers are represented as C2 agents.

B. Modeling

In the simulation sensor agents perform pre-defined formation movements until a target agent has been observed at which point they pass this information to the C2 agent after which a sensor agent may be chosen to track a target. At start up effector agents remain stationary in a randomly assigned location after which they may be assigned to a mission to capture targets. The movement of target agents is based upon a probabilistic mechanism, where all targets move according to a simple bounded random behavior model used in previous NITEworks [14] studies. NITEworks is a UK MoD program which has developed battlespace models to assess future military capability requirements. This research has utilized fragments of previous NITEworks models, where the tasking of sensors and effectors to specific missions (targets) is allocated by C2 for both centralized and decentralized scenarios. The principal difference between the centralized and decentralized models used here is the way in which sensor observations are correlated and reported to effectors. In the centralized model all sensor observations are correlated by C2, whereas in the decentralized model all sensor observations are autonomously correlated by individual sensors before C2 is notified for mission tasking. In the centralized model sensor observations are reported to effectors via C2, however in the decentralized model sensor observations are reported directly to effectors. As a result the decentralized model does incur additional latency delays during the mission tasking phase. This is due to the need for a credential negotiation task, where the C2 agent acts as a trusted third party providing credentials enabling sensors and effectors to mutually authenticate before sharing potentially sensitive information.

In the case of a centralized access control model the information exchange architecture consists of all agents connected through a central control station. Given this architecture any sensor observations of a targets latest location and velocity need to be communicated via the control station, as illustrated in fig. 2. Thus all agents have direct interaction with central command removing potentially inefficient intermediary processes, such as setting up a communications channel for individual interactions. However such a centralized model also assumes limited levels of self-capability, where all agents are treated as dumb end-points which must communicate through an intelligent central process. From an information security and in particular availability perspective the centralized model also reduces the resilience of the system to failure or attack due to a potential single point of failure at the C2 node. In the centralized model all sensor observation correlation and target track messages receive the highest priority in the queuing system; thus minimizing processing delays due to the C2 agent.

A decentralized access control model enables an ad-hoc and distributed information exchange architecture, where individual sensor and effector agents can securely interact and share observations on target agents, as illustrated in fig. 2. This introduces the potential for a swarm-like MANET, which can meet high-level operational objectives with minimal external intervention. In the decentralized model sensors correlate observations locally, this could potentially reduce the load on the C2 node and improve the overall operational performance. All latest target track data is sent directly from the sensor to the effector in the decentralized model, this is unlike the centralized model in which all interactions between non–C2 agents must go via C2. The decentralized model does have additional delays representing credential negotiation between the C2 and sensor/effector agents for each mission assignment. This is modeled as the delay between both a sensor and effector receiving tasking details to pursue a particular target for a given mission, which subsequently impacts on a sensors ability to feed target track data to an effector. Ultimately such delays influence the effectors ability to capture a target. For the decentralized model security credential negotiation latencies result in a delay which is on average ten times that of the centralized model. Such credential negotiation is required to ensure that sensors and effectors can authenticate and therefore authorize the sharing of information services such as the targets latest location.

The aim of the simulation is therefore to quantify the benefits (or otherwise) of decentralized information exchange over the currently implemented centralized architecture. This is achieved by assessing the time taken from a targets initial identification to its capture (Total Capture Time), for different values of the Deliver Target Effect (DTE) and Emit Target Stimulus (ETS) tasks. The DTE task represents the final capture phase of a target by an effector, whilst ETS is the sensor observation refresh rate, which determines the freshness of target track data.

As described previously in the centralized model target tracks are reported by sensor to effector agents via C2, whereas in the decentralized model sensors report target tracks directly to effector agents. Therefore to assess the impact of communications link latency on the performance, three different ratios of sensor/effector to C2 and sensor to effector communications link latencies are tested (1:1, 5:1 and 40:1).

In the model individual tasks and communications links are subject to latencies which could be due to any number of factors such as throughput, terrain and jamming. Details on the characteristics of each task and individual parameter values used are beyond the scope of this paper. However it is worth noting that average latencies with corresponding probabilistic distributions (associated with each agent type for the processing of individual tasks) and parameter values such as those assigned to both DTE and ETS are based upon standard battlespace modeling practices as in [14]. This enables the accurate assessment of an effectors ability to successfully capture a target. The model developed outputs log data in the form of .csv files which can be opened as Microsoft Excel sheets.

IV. Results

A. Findings

As suggested previously the scenario was tested for a range of values (0.5 to 9.0 with increments of 0.5) for DTE and ETS, where each test was run for the equivalent of 4320 minutes (or 3 days). In fig.'s 5 and 6 Dec represents the decentralized network and Cen1, Cen2 and Cen3 represent centralized networks with communications latencies of 1:1, 5:1 and 40:1 respectively.

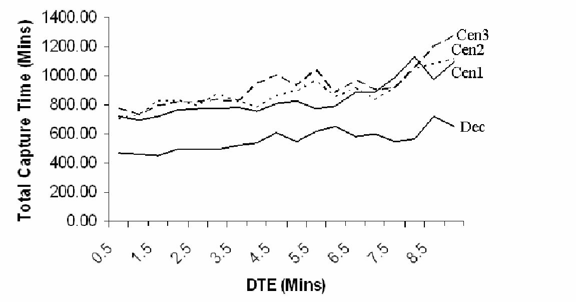


Fig. 5. Average time taken to capture a target when DTE is varied for centralized and decentralized information sharing.

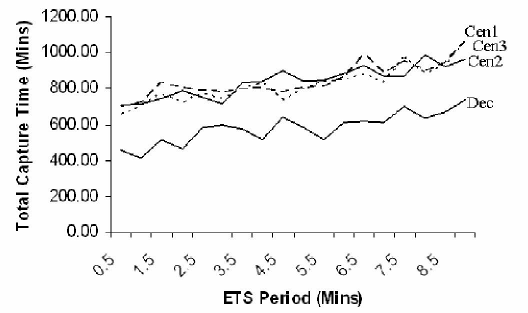


Fig. 6. Average time taken to capture a target when ETS is varied for centralized and decentralized information sharing.

B. Analysis

The results from the tests undertaken are given in fig.'s 5 and 6 respectively, from which it can be seen that there is a steady increase in the Total Capture Time (performance) as both the DTE and ETS parameter values increase. Even when the latencies of sensor/effector to C2 and sensor to effector communications links are equal, the decentralized model (Dec) provides superior performance, enabling more timely capture of target agents. This is in the presence of an extremely high average delay for mission tasking in the decentralized model due to security credential negotiation. Although the performance of the centralized model can be seen to improve with better communications links between C2 and sensor/effector agents, there is still a significant difference in average performance between centralized and decentralized solutions. The average performance difference is calculated as follows,

$$Average\ \ Difference = \frac{\sum_{x=0.5}^{9.0} \sqrt{(Dec_x - Cen_x)^2}}{18} \tag{1}$$

where Dec_x and Cen_x give the Total Capture Time values for a decentralized and centralized test and x represents ETS or DTE. The sum of all such differences is then divided by 18 which is the total number of tests giving the average.

For both parameters DTE and ETS the best performing (minimum average difference) centralized solution is Cen1, however even this, results in significant differences (ranging from ~40% to ~60%) in Total Capture Time between Dec and Cen1 for both DTE and ETS. It is believed this is due primarily to the delays in the sensor correlation task, which in the centralized model is reliant upon C2 to coordinate and correlate observations in contrast to the decentralized model, where sensor agents correlate observations autonomously. Underlying this reduced performance in the centralized models is the bottleneck in queuing and therefore processing of target observations, which occurs at the C2 agent resulting in a decay of its ability to execute operations.

In this experiment the shared data (i.e. target location tracks) was both small and fixed in size. However future work may consider data of larger and differing sizes such as image or video files of a target to confirm capture. In such cases the performance of the decentralized model may decrease if the bandwidth of the sensor to effector link is less than the sensor/effector to C2 link.

V. Candidate Access Control Architecture

A. Beyond Identity Access Control

In order to achieve the potential benefits of decentralized information sharing outlined in section IV individual agents must be capable of making authorization decisions; therefore we propose an alternative to the current centralized electronic access control model. Traditionally electronic access control privileges and therefore decisions have been based upon identity alone, where a list of agent identities authorized to access a service is pre-defined, the most prevalent access control model is known as an Access Control List (ACL).

In a MANET where M2M interaction are likely to be prevalent, access control based upon identity alone is likely to inappropriately reflect an agents need and authorization to access services. For example to form an ad-hoc coalition two or more agents may need to securely share sensitive services such as location information in a decentralized manner, in such scenarios authorizations for specific agents with respect to specific information services may evolve. Such authorizations may be dependent upon other attributes as well as identity. In particular the temporal and geographic location of an agent as well as available bandwidth may be used to more accurately control information exchanges. Therefore contextual factors may be used as additional constraints, enabling fine-grained decentralized access control. The potential for this form of context-aware computing (or location-based services) [15]–[17] to be used as an access control mechanism has also been identified in, [18]–[21].

B. Context-Dependent RBAC

As part of our proposed security architecture Role-Based Access Control (RBAC) has been chosen, to control an agent's access to information services. This is due to the efficiency advantages of RBAC over Discretionary (DAC) and Mandatory Access Control (MAC) models as described in [22]. In previous RBAC models [22] privileges have consisted of operations such as read and write with respect to some object, whilst work in the context-aware access control field has focused on dynamically adjusting the privileges assigned to an agent based upon contextual factors. An example of such context-aware access control is Zhang and Parashar's work [18] on Dynamic Context-Aware Role-Based Access Control (DRBAC). The DRBAC model extends traditional RBAC [22], by dynamically adjusting roles and privileges associated with agents according to contextual factors such as an agent's current location. However this introduces significant overhead as well as complexity such as the possibility for conflicts [18] between an agents current and previously assigned privileges. Therefore we propose to use traditional RBAC$_1$ introduced by Feinstein et al. [24] as a mechanism to administrate and not dynamically adjust context-dependent privileges, where the context-dependent privilege builds upon traditional privileges by incorporating time and location as additional constraints on the operation.

Context-dependent privileges incorporating temporal and geographic constraints were introduced in [5] as an Authorization State (AS), the proposed incorporation of this into the overall RBAC model is illustrated in fig. 7. An AS specifies the authorized location, time and operation for an agent to access a service. In a DDF application this could enable sensor agents to share situational awareness, for authorized geographic areas and times without compromising the security principle of least privileges and removing the need for authorization via a central control station. In an organizational environment it is possible to predict the services required by agents fulfilling specific roles, therefore AS's can be pre-assigned to different roles.

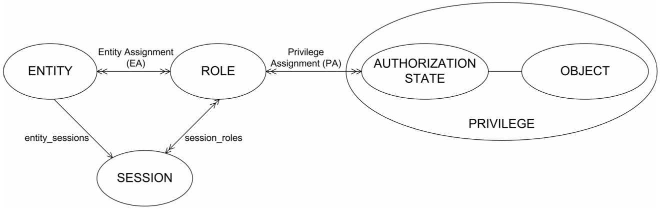


Fig. 7. Introduction of AS mechanism into the core RBAC model.

C. Achieving Context-Dependent RBAC

As described previously an AS specifies the temporal, geographic and operational (read, write etc.) attribute constraints which are assigned to a given privilege, this is based upon the Attribute Certificate (AC) introduced by Farell and Housley in [25]. An AC is a digital certificate based mechanism which can be used for both authorization as well as authentication purposes. A separate AS is assigned to an agent for every service the agent is authorized to access, where RBAC enables the efficient assignment of AS's to agents. In our architecture it is proposed to use the EureCA certificate to implement the concept of an AS. EureCA certificates were introduced in the Mobile Workers' Secure Business Applications in Ubiquitous Environments (MOSQUITO) program [26] as a combined authentication and authorization credential. The EureCA certificate uses an XML schema to describe a PKI based certificate which must be digitally signed by an authority trusted by the service provider, this could be used as the basis of federated identity techniques such as Security Assertion Markup Language (SAML). An example AS format is given in fig. 9 (see Appendix), where it can be seen that as well as including the public key for authentication of identity the AS also includes the temporal and geographic constraints within which an agent may access a specified service.

To date the literature on context-aware access control [18], [21], [26] has focused on credential pull type systems with centralized authorization. In credential pull systems the service provider (policy enforcement point) requests the necessary policies and credentials for a client from a trusted third party (policy decision point). Similarly centralized authorization requires the service provider to refer a clients request for service to a remote decision point, which consults a central policy store. Both credential pull and centralized authorization based systems assume significant infrastructure. However in ad-hoc environments such as those envisaged and considered in the SEAS DTC [1] and ALADDIN [2] projects, MANETs will need to operate with high degrees of autonomy with minimal infrastructure deployments. Therefore a credential push type access control system has been chosen, which enables local (or distributed) authorization decisions to be taken by service providers. Using the push based system the client provides all the necessary credentials (EureCA certificates) to the service provider, the service provider can then make local authorization decisions.

The use of a credential push based system with decentralized authorization, improves the autonomy (or self-management) of a MANET by reducing the reliance of individual agents' upon third parties for access control decisions and therefore information sharing. This means when an agent receives a request for service it can locally process this assuming the consumer provides the necessary credentials (e.g. digitally signed certificate from a mutually trusted party). A high level illustration of the differences between decentralized push and centralized pull access control systems is given in fig. 8. Actions 2a and 2b are additional requirements of the centralized model as it needs to acquire the credentials (for authorization) of a client after authentication. A benefit of the centralized model is that policies can be implemented without changes to the client and server; however of more importance in this instance is that the centralized model incurs additional performance costs due to the servers need to pull credential information in real-time. To overcome the compromise of an agent(s) it is proposed to use the periodic dissemination of a black list, although a strategy to detect compromise has not yet been derived. Additional protection is provided though the use of ephemeral digital certificates.

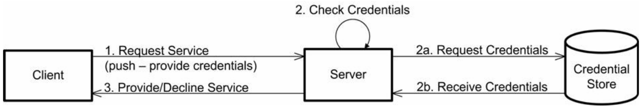


Fig. 8. Decentralized and centralized authorization for credential push/pull.

Traditionally digital certificates have been used to authenticate an identity, by proving that a specified public key belongs to the claimant. This is illustrated in fig. 9 (see Appendix) through the presence of elements issuer and holder. In AS's this concept is expanded by including the attributes and service elements, where the attributes describe the constraints within which a given agent may access a service(s).

D. Formal Definition of Context-Dependent RBAC

The data elements which make up our context-dependent access control model and the relationships between these are illustrated in fig. 7. This is based upon the RBAC model presented in [22]. It can be seen that an agent a∈AGENT is assigned to one or more roles r∈ROLE and a role can be assigned to one or more agents. A session s∈SESSION is a mapping between an agent and an activated subset of roles that are assigned to that agent at a given point in time. An active role is associated with one or more privileges p∈PRIVILEGE, where p is an approval for an agent to exercise an authorization state on one or more services se∈SERVICE. An authorization state as∈AUTHORISATION STATE specifies the temporal (t∈TIME), geographic (l∈LOCATION) and operational (o∈OPERATION) constraints (read, write etc.) which are associated with a given privilege with respect to a specific information service se. Abstractly many authorization states can be associated with many services and similarly many services can be associated with many authorization states.

Fig. 7 also illustrates Agent Assignment (AA), Privilege Assignment (PA) and Role Hierarchy (RH) relations; these relations are fundamental components of RBAC. There are also two primary functions which relate to sessions, where each session is associated with a single entity and each entity is associated with one or more sessions. The function session roles represents the roles activated by the session and the function agent sessions represents the set of sessions that are associated with an agent. The privileges available to an agent are the privileges assigned to the roles that are activated across all of an agents sessions. The proposed access control model can be summarized as follows:

- AGENT, ROLE, SESSION, AUTHORISTION STATE, PRIVILEGE and SERVICE.
- AR $\subseteq$ AGENT×ROLE, a many-to-many mapping agent-to-role assignment relation.
- AS $\subseteq$ TIME×LOCATION×OPERATION
- assigned_agents(r) = {a$\in$ AGENT | (a,r)$\in$AR}, a mapping of role r onto a set of agents.
- PRIVILEGE: AUTHORISATION STATE$\leftrightarrow$SERVICE, the set of privileges.
- PA $\subseteq$ PRIVILEGE×ROLE, a many-to-many mapping privilege-to-role assignment relation.
- assigned_privileges (r) = {p$\in$PRIVILEGE | (p,r)$\in$PA}, mapping of role r onto a set of privileges.
- (p: PRIVILEGE) $\rightarrow$ {(as,se) $\subseteq$ PRIVILEGE}, the privilege-to-authorization state mapping, which gives the authorization state and service associated with privilege p.
- agent_sessions (a: AGENT) $\rightarrow$ {S $\subseteq$ SESSION}, mapping of agent a onto a set of sessions.
- session_roles (s$\in$S) = {r$\in$ROLE | (agent_sessions (a), r) $\in$ AR}, mapping of session s onto a set of roles.
- $\bigcup_{r \in session\_roles} assigned\_privileges(r)$, the privileges available to an agent in a session.
- RH $\subseteq$ ROLE×ROLE is a partial order on ROLE called the inheritance relation, written as $\geq$, where $r_1 \geq r_2$ only if all privileges of r_2 are also privileges of r_1, and all agents of r_1 are also agents of r_2. This is reflected in the fact that agents higher up the organization hierarchy have the privileges to view the SA information available to subordinates.

In the formal definitions above, EA defines the relationship between entities and roles; PA defines the relationship between privileges (including authorization states) and roles. RH defines the inheritance relationship between roles and implicitly privileges. The principal difference between the context-dependent RBAC model described here and that of the original RBAC model in [22] is the use of an AS instead of a basic operation (read, write, execute etc.). This enables more fine grained electronic access control.

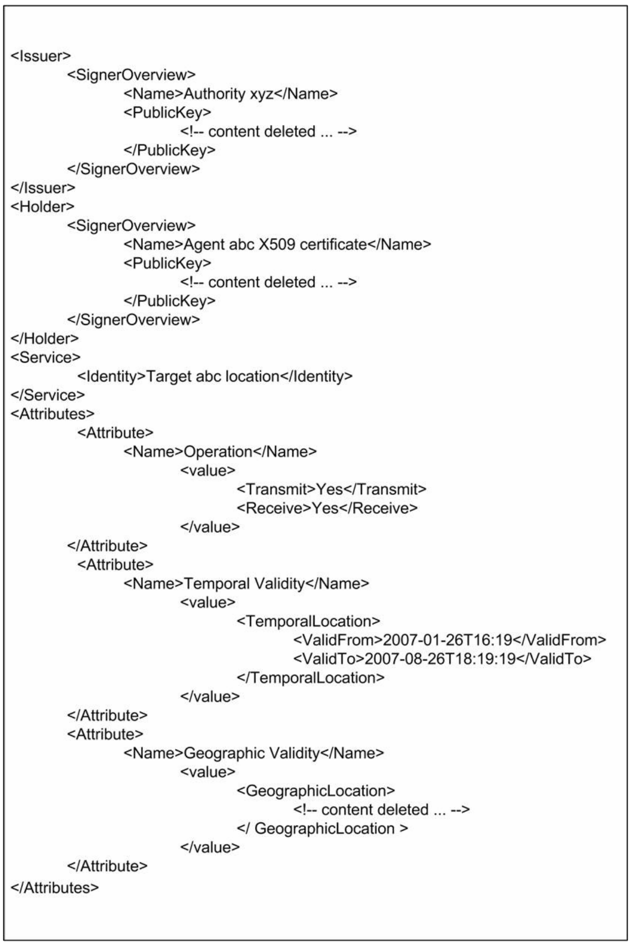
VI. Conclusions and Future Work

Ubiquitous computing is being facilitated by concepts such as MANETs, in which a group of mobile devices (or agents) collaborate by interacting and sharing services in a distributed and ad-hoc fashion. In order to enable this, individual agents must be capable of automatically making access control decisions in a local and decentralized manner. This is in contrast to current practices which require centralized human based mechanisms, to control the flow of information to and from individual agents. Through modeling, this paper has highlighted the operational benefits of decentralized over centralized access control for a HLS scenario, in which a MANET consisting of a collaborating group of autonomous agents need to share information to capture targets as soon as possible. From the modeling it has been found that decentralized information sharing enabled by an appropriate access control model, performs significantly better than corresponding centralized information sharing techniques due to a communications and processing bottleneck at C2 in the centralized model. This is true even when expensive minimal latency communications links are employed between agents in the centralized model and the decentralized model is penalized by the introduction of delays in information sharing due to security credential negotiation. Future modeling is suggested to assess the breakpoints in performance when data of larger and differing sizes such as image or video files of a target are shared.

A candidate context-dependent RBAC model has also been proposed to enable decentralized information sharing. Experimentation and evaluation of this proposal in an analogous fashion to the experiment described in this paper is needed. In the future the proposed model may be implemented in the Configurable Systems Engineering Research Tool (ConSERT)[2], which is a MANET developed by BAE Systems. In this paper a distinction between context-dependent and context-aware access control has been made, where context-aware access control policies require real-time verification of contextual attributes, such as an agents location. Therefore context-dependent RBAC has been offered as a lightweight alternative, however in reality it is likely that a mixture of both context-dependent and context-aware will be used in context-based access control models in the future. In order to deliver such an access control model much work still needs to be undertaken not least from an information semantics point-of-view, which will be required to automatically filter data using the novel access control methods described in this paper.

[2] Consists of a number of autonomous agents, including an airship and ground vehicles.

APPENDIX



```
<Issuer>
        <SignerOverview>
                <Name>Authority xyz</Name>
                <PublicKey>
                        <!-- content deleted ... -->
                </PublicKey>
        </SignerOverview>
</Issuer>
<Holder>
        <SignerOverview>
                <Name>Agent abc X509 certificate</Name>
                <PublicKey>
                        <!-- content deleted ... -->
                </PublicKey>
        </SignerOverview>
</Holder>
<Service>
         <Identity>Target abc location</Identity>
</Service>
<Attributes>
         <Attribute>
                <Name>Operation</Name>
                        <value>
                                <Transmit>Yes</Transmit>
                                <Receive>Yes</Receive>
                        </value>
        </Attribute>
         <Attribute>
                <Name>Temporal Validity</Name>
                        <value>
                                <TemporalLocation>
                                        <ValidFrom>2007-01-26T16:19</ValidFrom>
                                        <ValidTo>2007-08-26T18:19:19</ValidTo>
                                </TemporalLocation>
                        </value>
        </Attribute>
        <Attribute>
                <Name>Geographic Validity</Name>
                        <value>
                                <GeographicLocation>
                                        <!-- content deleted ... -->
                                </ GeographicLocation >
                        </value>
        </Attribute>
</Attributes>
```

Fig. 9. Example AS certificate.

ACKNOWLEDGMENT

The authors would also like to thank Chris Coles, Richard (Dick) Elder, Robert Johnston, Paul Kimber, John Whitby and Chris Wood for their invaluable contribution to this work.

REFERENCES

[1] SEAS DTC, (2007, April 11), [Online] Available: http://www.seasdtc.com/

[2] Aladdin, (2007, April 11), [Online] Available: http://www.aladdinproject.org/

[3] J. Sandhu, A. Agogino, and A. Agogino, “Wireless Sensor Networks for Commercial Lighting Control: Decision Making with Multi-agent Systems”, *In AAAI Workshop on Sensor Networks*, 2004.

[4] R. Tynan, D. Marsh, D. O’Kane, and G. O’Hare, “Agents for Wireless Sensor Network Power Management,” *In Proc. IEEE ICPPW Conf.*, 2005.

[5] Z. Hayat, J. Reeve, C. Boutle and M. Field, “Information Security Implications of Autonomous Systems”, *In Proc. 25th IEEE MILCOM Conf.*, 2006.

[6] A. Yavnai, "An Information-Based Approach for System Autonomy Metrics Part I: Metrics Definition", *In Proc. Performance Metrics for Intelligent Systems Workshop*, 2003.

[7] IBM Research, Autonomic Computing, (2007, April 11), [Online] Available: http://www.research.ibm.com/autonomic/

[8] J. Kephart and D. Chess, "The Vision of Autonomic Computing", *IEEE Computer,* pp. 41–50, 2003.

[9] V. Tewari and M. Milenkovic, "Standards for Autonomic Computing" (2006, April 11), *Intel Technology Journal*, Intel Corp., [Online] Available: http://www.intel.com/technology/itj/2006/v10i4/3-standards/1-abstract.htm

[10] D. Alberts, J. Garstka and F. Stein, “Network Centric Warfare: Developing and Leveraging Information Superiority”, 2nd ed., *C4ISR Cooperative Research Program*, Washington DC: Library of Congress, 2000.

[11] IBM Research, “An Architectural Blueprint for Autonomic Computing” (2007, April 11), IBM Corp., [Online] Available: http://www-03.ibm.com/autonomic/pdfs/AC_Blueprint_White_Paper_4th.pdf

[12] Wikipedia on Autonomic Computing (2007, April 11), [Online] Available: http://en.wikipedia.org/wiki/Autonomic_Computing

[13] Octatron Inc., SkySeer (2007, April 11), [Online] Available: http://www.octatron.com/prodSkySeer.html

[14] NITEworks, (2007, April 11), Online] Available: http://www.niteworks.net/publications

[15] G. Chen and D. Kotz, “A Survey of Context-Aware Mobile Computing Research”, *Technical Report TR2000-381*, Computer Science Department, Dartmouth College, New Hampshire, USA, 2000.

[16] P. Coppola, V. Della Mea, L. Di Gaspero, S. Mizzaro, I. Scagnetto, A. Selva, L. Vassena and P. Z. Riziò, “Information Filtering and Retrieving of Context-Aware Applications Within the MoBe Framework”, *Proc.of Workshop on Context-Based Information Retrieval*, Paris, France, 2005.

[17] A. Smailagic, D. P. Siewiorek, J. Anhalt, F. Gemperle, D. Salber and S. Weber, “Towards Context Aware Computing: Experiences and Lessons”, *IEEE Intelligent Systems*, pp 38-46, 2001.

[18] G. Zhang and M. Parashar, “Dynamic Context-Aware Access Control for Grid Applications”, *IEEE/ACM Int’l Workshop on Grid Computing*, Nov. 2003.

[19] J Hu, A C Weaver "A Dynamic, Context-Aware Security Infrastructure for Distributed Healthcare Applications", *Proc. First PSPT Workshop*, 2004.

[20] A. Toninelli, R. Montanari, L. Kagal, and O. Lassila, “A Semantic Context-Aware Access Control Framework for Secure Collaborations in Pervasive Computing Environments”, *Proc. Int’l Conf. Semantic Web*, Nov. 2006.

[21] S. Yokoyama, E. Kamioka and S. Yamada, “An Anonymous Context-Aware Access Control Architecture”, *Proc. International Workshop on Managing Context Information and Semantics in Mobile Environments*, 2006.

[22] S. Gavrila, D. R. Kuhn, D. F. Ferraiolo, R. Sandhu and R. Chandramouli, “Proposed NIST Standard for Role-Based Access Control”, *ACM Trans. Information and System Security*, pp. 224–274, 2001.

[23] J. Barkley, D. Ferraiolo and D. Kuhn, “A Role Based Access Control Model and Reference Implementation within a Corporate Intranet”, *ACM Transactions on Information and System Security*, pp. 34–64, 1999.

[24] H. Feinstein, R. Sandhu, E. Coyne and C. Youman, “Role-Based Access Control Models”, *IEEE Computer*, pp. 38–47, 1996.

[25] S. Farrell and R. Housley, “An Internet Attribute Certificate Profile for Authorization”, *Internet RFC 3281*, 2002.

[26] MOSQUITO Consortium, “Specification of Context-Sensitive Security Infrastructure”. 2005.

Zia Hayat was born in Darwen, Lancashire, UK in 1982 and graduated from UMIST, UK in 2003 with a 1st Class BEng. (Hons.) from the Department of Electrical & Electronic Engineering.

He is now completing an Engineering Doctorate (DEng.) in the School of Electronics & Computer Science, Faculty of Engineering at the University of Southampton, for this he is sponsored by BAE Systems and EPSRC, UK. Having worked on numerous computing and communication systems projects Zia is currently tasked with identifying and researching the key electronic security implications in the UK MoD's SEAS (Systems Engineering for Autonomous Systems) DTC (Defense Technology Centre) program. His main area of interest is information security risk management for ubiquitous computing. He has published and presented in various journals and conferences, including IET Information Security.

Mr Hayat is an active member of the IET, IISP, ISACA and ISSA and represents BAE Systems on various technology steering boards.