Semantic Web-based Access Control in Wireless Mesh Networks

Ghassan Chaddoud
Department of Scientific Services
Atomic Energy Commission of Syria
Damascus, P. O. Box 6091

ABSTRACT
In local communities, there exists a tendency to increase dependability on Wireless Mesh Networks, WMNs, as an appealing access network infrastructure, where municipalities and local communities would try to encourage information sharing and knowledge dissemination. However, WMNs are prone to different kind of threats such as disinformation and alteration, on one side, and their security would be overseen by local governments and citizens, on another side. This paper presents a new scheme to control access to WMNs based on semantic web techniques where information about people is available on the network for others, and people have knowledge of each other within their communities.

General Terms
Computer Science, Information Security, Network Security.

Keywords
Wireless mesh networks, Access control, semantic web, trust network, Trust ontology.

1. INTRODUCTION
Since Wireless Mesh Networks (WMNs) [1], as internet-working and access network technologies, are characterized by cost efficiency, ease of deployment and installation, municipalities and local governments could rely on these internetworking technologies as an *information dissemination platform* (IDP), with the aim of encouraging people to share information and boost knowledge dissemination and acquisition. In such internetworking environments, information could be easily disseminated, and localities' duties, such as training, educating, raising awareness, and the like, could be easily carried out. Furthermore, people could make use of them to present their experiences, knowledge, views, and opinions.

However, intruders might misuse the networks and use them as a step-off platform to launch diverse types of attacks, such as DoS attacks against information resources, or disseminate malign opinions or misleading information. Thus, in order for WMNs to form trustworthy information dissemination platforms, those internetworking environments must be protected against intruders. In addition, information about/from people should be reliable, and should not be misleading. Furthermore, in order to empower such networks and motivate people to invest in the affordable networking services and share their knowledge, information should be trustworthy and harmless.

At first thought, one could think of traditional security measures, such as shared secret-based user authentication; nevertheless, these measures are not suitable within the context of trustworthy information environments for many reasons. To start with, traditional security measures are expensive and affect the performance of applications. Secondly, given budgets constraints, municipalities would oversee WMNs protection. Thirdly, the lack of known effective semantic-based mechanisms that could be used to monitor disseminated information is a serious issue. Fourthly, as local citizens might be the sources of information, the usefulness and reliability of such information should be evaluated within certain contexts.

Given the aforementioned environments and in order to protect IDPs against intruders and disinformation attacks carried out by malign persons, access should be granted to users by the network operators and municipalities based on their contribution to and impact on the neighborhood.

The proposition to protect IDPs is based on the fact that individuals in local communities are supposed to know each other and their personal information are available on their social web pages. Furthermore, people themselves are able to play a role in controlling access to the network so as to ensure the security of their environments by forming webs of trust between entities that might be the sources of information or volunteering citizens.

A way to construct such webs of trust is semantic web techniques, where trust could be established among people, on the one side, and between individuals and the network operators, on the other side.

This paper proposes a new paradigm to control access to WMNs in local communities, where people can play a crucial role in evaluating the *integrity*, *reputation*, and *reliability* of others. A trust ontology is defined in order to represent and construct the web of trust. Depending on their integrity level, people are or are not allowed to get access to the networking services. People with an acceptable reputation level might evaluate the level of integrity and reliability displayed by others. Finally, the reliability level could be used to evaluate the expertise of the provenance of information and knowledge.

This paper demonstrates how to construct a web of trust using semantic web techniques and presents a scheme to control access to WMNs deployed in local communities. Section 2 overviews research works related to access control in WMNs. Section 3 illustrates how the IDP will be accessed and how entities interact with each other to protect the environment. Section 4 describes the system architecture. Section 5 describes a web of trust constructed using trust ontologies and used to control access to the WMN. Section 6 is a conclusion.

2. RELATED WORKS
To the best of our knowledge, there does not exist any semantic web-based access control proposed to control access

to WMNs. Moreover, the approaches proposed so far to control access to WMNs focused on user authentication, and can generally be classified as distributed and centralized. A distributed approach is characterized by the fact that a group of entities is responsible for authenticating clients. Usually, authentication functionalities are distributed over many dedicated nodes, called hereafter, distributed authentication servers. DASs. TUA [3], MeCA [4], and [5] are examples of such a class. In a centralized approach, such as 802.11s [2], ARSA [6], Mobisec [7], and AKES [8], one single entity, called authentication server, handles the authentication functionalities.

3. EXEMPLARY USE CASE SCENARIO

This section describes three use case scenarios that illustrate the roles of WMN nodes in the system, and how they interact to control access and organize services. In these scenarios, we assume that all WMN routers are peers and responsible for controlling access to services offered by the local government and citizens, WMN clients. These services are called hereafter local services. The first scenario is illustrated in Figure 1.

Firstly, **client access**. A client, *C1*, contacts an access router, *AR1*, requesting permission to get to networking services. Client *C1* is granted access permission if he/she has not been previously expelled or his/her integrity evaluation is acceptable, *i.e.*, not bad. A client might be expelled for many reasons such as harmful behavior towards his/her community and neighborhood. This includes cases where he/she is known for carrying out sabotage acts against networking services, or if his/her access request had already been rejected due to bad integrity evaluation.

To follow up on client *C1* request, *AR1* polls the WMN clients to evaluate client *C1*'s integrity by means of a trust evaluation mechanism. If the evaluation fails due to the fact that client *C1* is not honest for example, *AR1* rejects the request and inform the other access routers about client *C1*'s integrity evaluation results. Otherwise, *AR1* informs client *C1* that his/her request has been approved and is allowed to get into the networking services.

Secondly, **client contribution** to the provision of local services and other knowledge and information. WMN clients are allowed to share information and knowledge made available via (social) web pages or services such as consultancy, training and educational tutorials, and awareness courses proposed via web services.

Once a client, *C2*, has developed a content or a service, and wishes to make it available to the local community as part of the local services, he/she contacts an access router, *AR2* for instance, in order to make his/her contribution available to the public. Similarly to the first use case, *AR2* polls WMN clients to evaluate client *C2*'s reliability level. Depending on *C2*'s reliability evaluation results, *AR2* might reject *C2*'s request and notify the other access routers about C2's request rejection. Otherwise, C2's contribution should be added to the local services with his/her current reliability evaluation level.

Thirdly, **client participation** in protecting the IDP. Access routers need to cooperate with some WMN clients in order to evaluate other WMN clients' integrity and reliability levels. However, it is reasonable for the access router not to treat all WMN clients evenly. Since some WMN clients might manipulate public opinion, mislead people, or would misdirect them in order to serve their own interests. For these reasons, WMN clients who participate in evaluating others' integrity and reliability should be chosen carefully. At first, the access routers might be provided by local community administrations with a list of people how are known to be good citizens; honest, active within local communities, and have a good reputation. The access routers might then expand the list and their cooperation with other WMN clients after rigorous social and professional background scanning, or after going through an on-demand reputation evaluation process.

The latter case could be carried out in a similar way to the first two scenarios. When an access router, *AR3*, receives a request from a WMN client, *C3*, requesting approval to participate in protecting the IDP, *AR3* could ask for the opinions of the list members, and then *C3*'s reputation might be evaluated by means of a trust evaluation mechanism.

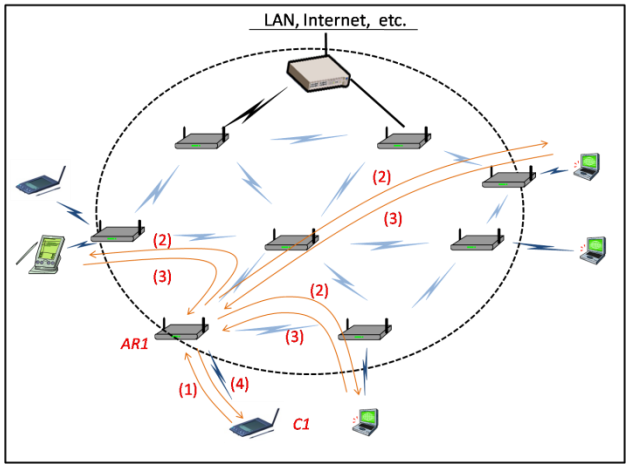

Figure 1. Use case Scenario. Client *C1* sends an access/participation request (1) to *AR1* who asks (2) other clients about *C1*. Clients send back their evaluation (3) to *AR1*. *AR1* informs (4) *C1* about the result of his/her evaluation that results in rejecting or approving his/her request.

4. SYSTEM ARCHITECTURE

The following subsections present the network, application, and trust models.

4.1 Network Model

The network model is composed of the following:

- A *mesh backbone infrastructure* composed of *mesh routers* and *mesh gateways*. While mesh routers are responsible for relaying data and granting access permission to *mesh clients* with the aim of sharing information and knowledge or getting networking services, gateways ensure interfacing with the Internet or other networks, as shown in Figure 1. The components of the infrastructure are assumed to be stationary;
- *Mesh clients* who are a single hop away from the mesh backbone and use it to connect to each other or to other networks. Although, clients might be mobile, they are assumed to be stationary at least during an access session. Moreover, they might be online all the time in order to share information, knowledge, and the like.

4.2 Application Model

A 4-tier application model is used, as illustrated in Figure 2.

- *Client-tier*: represents mesh clients who are interested in requesting access to networking services and the *content-*

tier. Clients are granted access permission based on their *integrity* level.

- Content-tier: formed of information and knowledge, and local services made available by mesh clients. Clients are granted permission in order to share information and provide services based on their reliability level. Although, local municipalities might participate in the content-tier as well, we restrict this work to the participation of mesh clients.
- Trust-tier: composed of mesh clients who are known to be involved in local community activities, and would be qualified to evaluate the integrity and reliability of other mesh clients. Trust-tier members are chosen based on their reputation.
- Access-tier: formed of some backbone routers, called hereafter access routers, and is responsible for:
    - Granting access permission towards *content-tier* or any other networking services.
    - Constructing *content-tier*. Access routers designate the mesh clients who are qualified to share information and knowledge, and provide *local services*.
    - Forming *trust-tier*. Access routers designate clients who are qualified to evaluate the *integrity* and *reliability* of other clients based on their *reputation*.

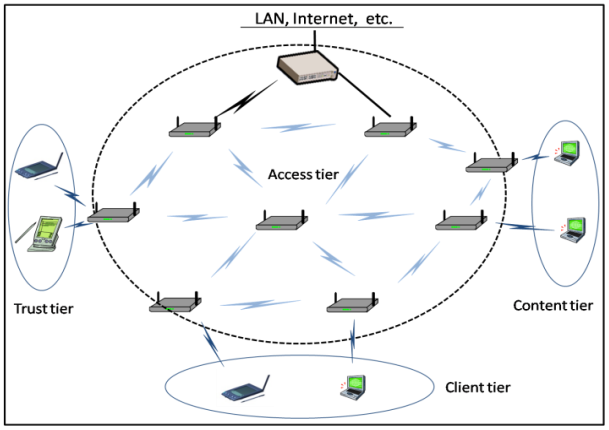

Figure 2. Access control architecture, with four tiers: *trust-tier*, *content-tier*, *client-tier*, and *access-tier*.

4.3 Trust Model

Since the aim of this paper is to create an open trustworthy environment, we devise a WMN as an Information Dissemination Platform (IDP) so as to share information, knowledge, and training services useful to local community citizens, and we propose to control access to the WMN by constructing a web of trust.

The web of trust is built amongst mesh clients belonging to the *trust-tier*. When a client asks for access permission to the network, access routers send a query to the *trust-tier* in order to evaluate mesh clients' integrity, reliability, and reputation levels.

Since the focus is on offering services to local communities' citizens, the access routers are assumed to be reliable and trustworthy to carry out the tasks entrusted in their tier, and their security is beyond the scope of this work. Further, a trust relationship is assumed to be in place amongst those routers. Furthermore, it is assumed that, at the beginning of the provision of local services, all mesh clients are eligible for access networking services.

In addition, it is assumed that a mesh client in the *trust-tier* is able to evaluate the integrity, reliability, and reputation levels of some other clients by means of direct or indirect acquaintance. In addition, these evaluations are used when access routers poll them with the aim of evaluating a mesh client's integrity, reliability, and reputation levels.

Finally, it is assumed that access routers store information about dishonest clients and are trusted to exchange their findings with others.

5. TRUST ONTOLOGY

In the first subsection, we build a web of trust using a trust ontology that is used to describe and represent relationships amongst WMN clients. The second subsection serves as an algorithm to evaluate trust levels of mesh clients.

5.1 Building the Ontology

The ontology built in this paper is a simpler version of Golbeck's ontology [9]. In the following, the trust ontology is constructed according to the methodology illustrated by Nima in [12].

- **Domain and scope determination**. The focus is on the representation of trust relationships amongst persons, mesh clients, in the local community. The ontology is going to be formed around trust, relation, local community, and semantic web.
- **Data Learning**. Information about people and their relationships and related evaluations is assumed to be available on their web pages' profiles, and described within FOAF [10] files. Hence, data of the ontology is formed of information, existent within WMN clients' profiles, about peoples' trust relationships and their properties, in addition to metrics qualifying trust relationships.
- **Task definition**. The task of the trust ontology is to represent and describe trust relationships amongst the local community's citizens, mesh clients, in order to evaluate WMN clients' trust levels.
- **Ontology learning**. There are two main concepts in our ontology: Person and Trust. A person who would be a mesh client stores a list of his/her acquaintances in his/her neighborhood along with their trust levels. A trust level is assigned locally by the profile owner and used to express his/her belief regarding the integrity of the acquaintance, the subject of evaluation. The trust level can take on one of the values {1, 2, 3, 4, 5, 6, 7, 8, 9}, adopted from [11]. The values correspond to the following:

1. Distrusts absolutely
2. Distrusts highly
3. Distrusts moderately
4. Distrusts slightly
5. Trusts neutrally
6. Trusts slightly
7. Trusts moderately
8. Trusts highly

9. Trusts absolutely

A person "Distrusts absolutely" one of his/her acquaintances if he/she knows that the latter has carried out harmful actions against networking services or WMN clients in his/her local community. A person "Trusts absolutely" one of his acquaintance if he/she knows the latter as a good person and would do nothing harmful to his/her community. The other values are interpreted at the user's discretion.

5.2 Trust Inference

When a WMN client, *C1*, requests access to the networking services, his/her access router *AR1*, the one who receives the request, has to decide whether the client is or is not eligible for accessing the network. As mentioned above, if the information available to *AR1* indicates that the client is dishonest or blacklisted then *AR1* should reject client *C1's* access request. Otherwise, a trust evaluation procedure starts. This procedure is based on the web of trust constructed so far and consists of the following:

AR1 sends queries to the web of trust in order to get a trust evaluation of client *C1*. The request is directed to *C1*'s neighbors. If a *C1*'s neighbor had an answer then he/she would send it to *AR1;* otherwise, the neighbor queries the web of trust, and a trust value is calculated according to the following:

For any neighbor who is not directly connected to *C1* within the web of trust, the trust value is determined by a weighted average of the values of each of his/her neighbors who have a path to *C1*. The calculated trust *t* from node *i* to node *s* (*C1*) is given by the following recursive function:

$$t_{is} = \frac{\sum_{j=1}^{n} \begin{cases} t_{ij}\, t_{js} & if \;\; t_{js} \geq t_{ij} \\ \left(t_{js}\right)^2 & if \;\; t_{js} < t_{ij} \end{cases}}{\sum_{j=1}^{n} t_{js}}$$

Where *n* is the number of *i's* neighbors with paths to *C1*. This formula is a variant of the one proposed in [11], and ensures that *C1*'s neighbors are trusted more than those who are closer to *AR1*.

Once *AR1* gets the evaluations of *C1's* trust values, it averages the values, and if the answer is smaller than 5, then *AR1* considers that *C1* is not honest and rejects his requests. Otherwise, *AR1* informs *C1* that her/his request has been approved and can go further in the association with *AR1*.

6. CONCLUSION

Security of WMNs based on traditional security mechanisms, such as MAC and digital signatures, seems to be inappropriate in certain configurations, where the focus is on the common public benefits rather than those of the network operators. In this paper, a new paradigm is introduced to control access to WMN-based networking services in local communities.

Access to the WMN is granted to WMN clients based on their trust evaluations. The evaluation is carried out within a web of trust constructed using a trust ontology. A WMN client would not be granted permission without the approval of the majority of his neighbors.

The focus in this paper is on the proposal itself as a proof-of-concept of a new access control paradigm. However, a security analysis should be carried out to test its resistance against malign user attacks and other types of attacks. Furthermore, a test-bed is required to evaluate the impact of the security solution on the network performance, especially, on the time required for WMN clients to become associated with their respective access routers.

Finaly, the application domain of this new access control scheme might be world wide specific-purpose social networks.

7. REFERENCES

[1] Akyildiz, I. F., Wang, X., and Wang, W., "Wireless mesh networks: a survey", Computer Networks, vol. 47, pp. 446–487, 2005.

[2] IEEE 802.11s Task Group, Amendment: ESS Mesh Networking, D3.0.

[3] Lin, X., Lu, R., Ho, P.H., Shen, X. and Cao, X., "TUA: A Novel Compromise-Resilient Authentication Architecture for Wireless Mesh Networks", IEEE Transactions on Wireless Communications, vol. 7, no. 4, April 2008.

[4] Kim, J. and Bahk, S., "Design of certification authority using secret redistribution and multicast routing in wireless mesh networks", Computer Networks, vol. 53, issue 1, 2009.

[5] Yang, K., Jia, X, Zhang, B. and Zhongming, Z., "Threshold Key Redistribution for Dynamic Change of Authentication Group in Wireless Mesh Networks", in Proceedings of GLOBECOM'10, 6 – 10 Dec, Miami, Fl, 2010.

[6] Zhang, Y. and Fang, Y., "ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks", IEEE Journal on Selected Areas in Communications, pp. 1916 – 1928, 2006.

[7] Martignon, F., Paris, S., and Capone, A., "MobiSEC: A Novel Security Architecture for Wireless Mesh Networks," in Q2SWinet, 27 – 31 Oct, Vancouver, Canada, 2008.

[8] He, B., Joshi, S., Agrawal, D.P. and Dongmei, S., "An Efficient Authenticated Key Establishment Scheme for Wireless Mesh Networks", in Proceedings of *GLOBECOM'10*, 6 – 10 Dec, Miami, Fl, 2010.

[9] J. Golbeck J., Parsia B., and Hendler J., "Trust Networks on the Semantic Web", ISSU 2782, pp. 238-249, Lecture Notes in Computer Science – Springer, 2003.

[10] Brickley D., and Miller L., "FOAF Vocabulary Specification, Namespace Document", September 2, 2004, Available at: http://xmlns.com/foaf/0.1/

[11] Golbeck J., "Inferring Trust Relationships in Web-based Social Networks", ACM Transactions on Internet Technology, Vol. 7, No. 1, 2006.

[12] Dokoohaki N., and Matskin M., "Effective Design of Trust Ontologies for Improvement in the Structure of Socio-Semantic Trust Networks", International Journal On Advances in Intelligent Systems, vol 1, no 1, 2008.