White Paper - WiNeMO Security Provision

Executive Summary

By Jonathan Loo, School of Engineering and Information Sciences, Middlesex University, UK

The future networks are envisioned to incorporate a large number of autonomous wireless objects moving with diverse mobility patterns while communicating via different radio interfaces. The moving objects range from personal wireless devices to wireless sensors such as RFIDs (radio frequency identification systems), carried by humans, vehicles, or unmanned aerial vehicles. These devices will give raise to new types of wireless and cellular networks. The envisaged applications include use in military, home, inventory control, environmental and medical monitoring, and space exploration. To the extent that these networks are truly different than existing forms of popular wireless networking, we can predict that the security challenges related to their use will also be different.

Wireless moving objects are constraint in radio range/coverage, processing capability and battery life, and are likely to have uncertain mobility patterns which could lead to dynamic changes in the network topology. The exceptional growth in mobile and wireless communications gives rise to serious problems of security at the level of the customer, network operator, and service provider. The causes of such rise, typically due to the fragility of the wireless link nature or the mobility features. Working in such dynamic wireless environments and with the resource-constraint devices makes the system by nature more vulnerable to a number of different security threats, from physical or logical attacks such as tampering or jamming; to abnormal behaviours that affect not only the performance of components inside the system, but also the confidentiality, privacy, authenticity, and integrity of the data. It is imperative to design network protocols with security considered at all layers as well as to arm the networks' systems and elements with well designed, comprehensive, and integrated attack defeating policies and devices. A fool proof prevention of attacks is challenging because at best the defensive system and application software may also contain unknown weaknesses and bugs. Thus, early warning systems (i.e. intrusion detection systems) as components of a comprehensive security system are required in order to prime the execution of countermeasures.

On the other hand, applications from many areas such as political, economic, financial or social standpoint strictly require the data to be secured, as well as assuring the robustness services at all times. Providing security in this context is therefore a crucial mission but not easy to solve. Information security services such as authentication, confidentiality, non-repudiation and access control are essential; however, the traditional mechanisms that provide these services are not enough due to the complex and dynamic nature of these new paradigms which bring more chances to the internal adversaries. For that reason, each infrastructure also has to be able to raise alerts or warnings in order to help both human users and the information subsystems to react against any possible anomaly that may downgrade or block their network services. Indeed, it needs a more systematic approach to build up a framework layout capable of allowing risk analysis of the threats and vulnerabilities of a mobile communication system, the assessment of a mobile communication system in terms of provided QoS and security, the protection of a service provided via mobile communication systems, and the engineering and management of mobile communication security. Moreover, an additional requirement for any security solution in this context is to be lightweight in order to save resources and extend the network lifetime. Developing energy efficient cryptographic is a major concern for the availability of these networks.

This white paper presents security problems and challenges of some specific domain areas relevance to WiNeMO. It offers expert opinions and guidance on the security provision where attentions and research are required. It is hope that its reading will stimulate interest and encourage researchers to continue investigate and evaluate new security solutions and approaches to enable future deployment of WiNEMO domain areas.

The following are the summary of the contributions provided by various domain area experts.

- **Security in M2M environments (see Page 3):** Machine-to-Machine (M2M) systems refer to pervasive environments where machines are active and can communicate with each other without requiring human intervention. The communication security is a critical enabler for the mass market adoption of M2M. End-

users demand that M2M communications achieve at least the same level of security as traditional human communications. In a digital context, confidentiality, integrity protection, privacy, authentication, and authorization are some of the key elements of security that need to be addressed in an end-to-end fashion. Efforts leading to standardization of M2M architectures are unfolding on a global basis, and the M2M security standards are being harmonized. The project raises the question of systematically addressing the security problems and characterizing the security infrastructure in such a system.

- **Authentication and certificate revocation in VANET (see Page 7):** Authentication is a must feature in VANETs as the source of the information should be verified to ensure the legitimacy of the data communicated. VANET applications typically have more stringent authentication requirements that distinguish them from wired networks: authentication should be done in real-time in VANETs to ensure enough time for the drivers to take action, a certain degree of anonymity is required to ensure privacy of drivers and authorized personnel should be allowed to lift the anonymity requirement for legal investigations. Among open problems that can be further investigated when providing authentication, revoking the credentials of misbehaving nodes is one of the most complex challenges. This project takes into account the issue of distributing large Certificate Revocation Lists in a reasonable time while optimizing the bandwidth utilization.

- **IDS countermeasures to protect QoS of 6LoWPAN from internal threats (see Page 11):** Internal threats are present in 6LoWPAN environments due to the fact that adversaries can tamper network devices and inject malicious code. Such threats will downgrade the network QoS and even block the operation of real time applications. This project assesses those internal attacks towards 6LoWPAN QoS and provides a potential solution based on an intrusion detection system (IDS) that combines a specification-based (RPL specification module) and an anomaly-based (statistical module) approach with some extended functions such as tracing back the malicious resource. By using a distributed architecture applied not only for the data collection, but also for the execution of the intrusion detection algorithm and the alarm correlation, the proposed IDS is able to prevent, counter, detect, and respond to attacks and potential threats.

- **Lightweight intrusion detection systems for wireless ad-hoc/sensor networks (see Page 15):** The IDS techniques need to be improved to deal with new attacks appearing day after day. On the other hand, to apply in WSN, they need to be lightweight due to the resource-constraint motes. This project offers a lightweight IDS solution, which is adapted to the context of WSN and has the ability of upgrading to detect the new coming threats, by applying human immune characteristics as guidelines. The system also benefits from cross-layer information to target a specific group of attacks. Using complex computations in parallel and decentralized patterns, the IDS can learn new information and recall learned information instantly, detecting invaders effectively. It can also learn the profile of normal activities and automatically distinguish them from attacks.

- **Lightweight security and privacy protocols formalization and reference architectures for WiNEMO (see Page 18)**: Because of the continuing need for lightweight authentication and key-exchange protocols, further research in this area has been done. Research on security solutions in resource-constraint environments always emphasises need for lightweight mechanisms, but how much lightweight is "lightweight"? This project clarifies the lightweight concept for such security (and privacy) solutions. The research also offers the metrics to estimate "lighweightness" and provides practical guidelines on how to build lightweight protocols for such resource-constraint environments.

A more elaborative material of the above topics are presented following this exclusive summary. Finally, I would like to extend my sincere thanks to all who have contributed their time and efforts in making this white paper a success. I am thankful to all the experts who have contributed their opinions research ideas and outcomes.

Acknowledgement

Thanks to AnhTuan Lee (MDX) and Carlos Gañán (UPC) who have offered views and opinions in the preparation of this exclusive summary.

Security in M2M environments

Jorge Granjal and Edmundo Monteiro
University of Coimbra, Portugal
{jgranjal, edmundo}@dei.uc.pt

1. Background and Motivation of security issues in M2M environments

Machine-to-Machine (M2M) systems promise to offer pervasive environments where machines are active and can communicate with each other without requiring human intervention. The M2M concept encompasses a combination of diverse heterogeneous electronic, communication and software technologies. In a M2M world there are sensors and actuators everywhere and such devices are able to communicate with each other and with devices on private networks or on the Internet. With a huge market expected for M2M devices and networks, M2M systems need to be properly developed and deployed. M2M technology will find applications in areas such as industry automation, smart spaces, home automation and healthcare, among many others [1]. This is also the vision of the Internet of Things (IoT), a world where ubiquitous and intelligent sensing applications contribute to a better and safer world. This vision may be materialized only if security is properly addressed from the start. Such applications will require a paradigm shift on how security is addressed, as we proceed to discuss.

2. Research challenges/Problem statements

Several characteristics envisioned for M2M applications will pose challenges to the design of security, in particular:

- Usage of heterogeneous communication technologies and protocols.
- Automatic communications between M2M devices without human intervention.
- Limitations on hardware capabilities of M2M devices.
- Expectations from users regarding privacy and liability.

Although many lessons and technical solutions may be inherited from results in research areas such as Wireless Sensor Networks (WSNs), M2M applications will require new approaches for security. M2M devices are expected to employ a myriad of wired and wireless technologies, such as Ethernet, GPRS, GSM, Bluetooth and IEEE 802.15.4, among several others. Protecting communications using such diverse technologies will require a careful evaluation of the adopted cryptographic algorithms or the design of new ones.

As communications may take place between M2M devices without the presence of a human, identification and authorization of M2M devices poses itself as a fundamental requirement. M2M devices may be mobile and for many scenarios a classic trusted third-party authentication scheme would not be appropriate.

Since many M2M sensing and actuating devices will be seriously limited in terms of computational capability, security technologies must be developed to cope with heterogeneous and constrained classes of devices. This implies that many existing security solutions may not be appropriate. Solutions involving the usage of infrastructures and the exchange of several messages related to security may be totally unfeasible for devices such as passive RFID tags.

Privacy and liability also appear as important aspects for M2M security. Users will require that systems allow the control of how much personal information is exposed, while on the other end certain applications will require that a certain degree of personal information is guaranteed to be available, for example in vehicular applications [2].

3. Proposed solutions, approaches, expert opinions and guidance

The previously identified challenges will require a paradigm shift in how many of the previous security issues are addressed. A security model for M2M applications will probably consider classic security solutions side-by-side with new decentralized and distributed security solutions, as in most scenarios a security infrastructure will not be available or desirable. In many scenarios M2M systems may be unable to derive definitive conclusions about the identity or intents of other devices. Therefore, security mechanisms may need to consider compromises between the need to enforce definitive security controls and the acceptance of controlled risks [2]. Security mechanisms may also be necessary that incorporate trust and privacy, two security requirements that will be cornerstone in M2M applications. Distributed and autonomous trust management and verification mechanisms will be required to support autonomous M2M device-to-device identification and authorization. Many M2M applications will also require the control of privacy and liability. For some M2M applications the user will require to be able to control the amount of personal information exposed to third parties, for instance in maintaining privacy while exposing personal records in healthcare applications. On the other end, other M2M applications may require that some of that information is available in case of necessity, for instance with M2M vehicular applications in case of traffic accidents.

3.1. Heterogeneous and constrained M2M devices

Regarding limitations on the computational capabilities of sensing and actuating devices, security technologies must be developed to cope with heterogeneous devices, some of which may be very limited. For example, applications using passive RFID tags are unable to support security mechanisms requiring the exchange of many messages and communications with servers on a security infrastructure. In this context, some solutions may already be available from research in areas such as Wireless Sensor Networks (WSNs). For example, several light weighted solutions for symmetric and asymmetric cryptography have been proposed in recent years. The introduction of security at the middleware of M2M applications or at the higher layers of the communications stack may be an approach to address the problem of securing communications using heterogeneous devices and communication technologies.

3.2. Identification, authorization and trust on M2M environments

Identification and authorization of M2M devices in a dynamic and autonomous world will pose serious challenges to research. Authentication mechanisms should work side-by-side with distributed trust management and verification mechanisms. Any two M2M devices should be able to build and verify a trust relationship with each other. Trust will be an important requirement for designing new identification and authentication systems for M2M.

As authentication is related with identification, M2M systems will probably need to incorporate some type of secure identifier, tying information identifying the device or application with secret cryptographic material. Current proposals are for the usage of X.509-based certified secure identifiers, for example using IEEE 802.1AR [3], or on the other end of self-generated uncertified secure identifiers. As M2M systems will require that privacy be balanced against disclosure of information, new authentication mechanisms making use of appropriate secure identifiers and incorporating privacy-preserving mechanisms need to be developed. This aspect may also be incorporated in new trust computation mechanisms, as the evaluation of the risk in accepting communications with a partially unknown device may also consider the level of privacy accepted for a M2M application. Three-way autonomous certification technologies can also provide a solution for authentication in the absence of an official certification.

As distributed and autonomous trust mechanisms will be required for M2M environments, trust must be established on the M2M device from the start. Local state control via secure boot (local trust validation) may be enforced for M2M devices. This secure boot may allow the establishment of a trusted environment providing a hardware security anchor and a root of trust, from which different models for trust computation

may be adopted. In this context, the Trusted Computing Group (TCG) [4] has proposed autonomous and remote validation models. Autonomous validation (using for example smart cards storing authentication secrets) presents the problem of requiring costly in-field replacements of compromised devices. Remote validation presents problems related to scalability and complexity, regarding limitations of M2M devices. The most promising avenue for research in this field may that of semiautonomous validation. Semiautonomous validation combines local validation with remote validation, meaning that a device is able to validate trust for another device and communicate with a trusted third-party in situations of absolute necessity (in many environments such third party may not be available at all). Distributed semiautonomous trust verification mechanisms are therefore necessary for M2M environments.

3.3. Anonymity and liability on M2M environments

As previously discussed, anonymity and liability are two interrelated security requirements for M2M applications. Such requirements are not only related with security, but also they are vital for the social acceptance of many applications envisioned for M2M. Anonymity is necessary as applications may only be accepted if the user is guaranteed to have a certain degree of protection of its personal (or other) information. Liability is a deeply related requirement, as other applications may require access to private information in case of necessity, for example for legal purposes. As anonymity will be required in M2M, research can target the applicability of light weighted formal anonymity models such as k-anonymity [5] to M2M environments. Possible alternative approaches are the development of mechanisms for data transformation and randomization. Intrusion detection will also be relevant for autonomous M2M environments. Autonomous and cooperative methods allowing the early detection of node compromises may be the path to follow in this domain [6].

3.4. Research and standardization on M2M

Research challenges must also consider the efforts of standardization on M2M. Technologies developed by standardization bodies need to address security from the start. Standardization is also important because M2M can replace proprietary technologies such as SCADA in the future. Unlike SCADA, M2M devices are able to push data to a server and M2M also works with standard technologies. Such factors will push towards the replacement of proprietary technologies with M2M solutions in the long term. This will open a huge market for M2M but also many security challenges. Regarding performance-constrained networks such as in industrial control environments, new MAC layers may be designed in order to benefit security. For example, TDMA approaches to MAC layer can incorporate reservations for security-related operations. This would allow security to be properly incorporated in M2M time-constrained critical environments.

Other standardization efforts that are important for M2M can be found at the IETF CoRE [7] and the ETSI M2M [8] groups, among others. Web scripting languages like XLM and web services will play an important part on M2M environments, because they facilitate the exchange of information between M2M devices and the communications of M2M devices with end users and applications. In this context, current proposals such as BiTXml [9] and M2MXML [10] would benefit from an analysis on security. This is also true considering current approaches on the adoption of RESTful-based communication solutions for M2M devices, for example the IETF Constrained Application Protocol (CoAP) [11], currently lacking security mechanisms.

3.5. Hardware-based security on M2M devices

Engineering and research challenges also reside in the design of new sensing platforms for M2M devices. A security co-processor may enable efficient cryptographic operations in low-end sensing and actuating platforms, as we can currently verify with result from research on WSNs. More complete hardware-based security solutions can also be used, such as the one currently proposed with Trustchip [12]. New platforms may be design to allow efficient computation of security algorithms appropriate to M2M applications. A related issue is the usage of secure storage mechanisms to store identification and secret security information

on a M2M device. This can be provided by a secure hardware-module with the characteristics of the Trusted Platform Module (TPM) proposed by the TCG [4] group. The usage of such a module allows the secure biding of the device identification and secret cryptographic information. As the usage of such hardware-modules may not be economically feasible, research should address the design of alternative software secure storage solutions and its impact on the overall security of M2M devices and applications.

4. Conclusions

Various characteristics of M2M devices and applications will demand a new approach on how security is addressed. The ubiquity and autonomous nature of many M2M applications will dictate that many security-related decisions are performed in the absence of a centralized and trusted security infrastructure. In this context, aspects such as autonomous communications between M2M devices, privacy and liability (among others) will pose major challenges to engineering and research. Many of the required security mechanisms will operate autonomously and in a distributed fashion. A security model for M2M may integrate solutions already proven to be appropriate to constrained environments with new security technologies developed for M2M environments.

5. References

[1] Inhyok Cha; Shah, Y.; Schmidt, A.U.; Leicher, A.; Meyerstein, M.V.; , "Trust in M2M communication," Vehicular Technology Magazine, IEEE , vol.4, no.3, pp.69-75, Sept. 2009.

[2] Du Jiang; Chao ShiWei; , "A study of information security for M2M of IOT," Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on , vol.3, no., pp.V3-576-V3-579, 20-22 Aug. 2010.

[3] IEEE 802.1AR, "Secure device identity", December 2009.

[4] Trusted Computing Group; http://www.trustedcomputinggroup.org/.

[5] Sweeney, Latanya, "k-Anonymity: A Model for Protecting Privacy," International Journal of Uncertainty, Fuzziness & Knowledge-Based Systems; Oct2002, Vol. 10 Issue 5, p557, 14p.

[6] Rongxing Lu; Xu Li; Xiaohui Liang; Xuemin Shen; Xiaodong Lin; , "GRS: The green, reliability, and security of emerging machine to machine communications," Communications Magazine, IEEE , vol.49, no.4, pp.28-35, April 2011.

[7] IETF Constrained RESTful Environments; http://tools.ietf.org/wg/core/.

[8] European Telecommunications Standards Institute M2M Communications; http://www.etsi.org/Website/Technologies/M2M.aspx.

[9] BiTXml, The ultimate m2m communication protocol; http://www.bitxml.org/.

[10] M2MXML, Open-standard XML based protocol for Machine-To-Machine (M2M) communications; http://m2mxml.sourceforge.net/.

[11] Z. Shelby, K. Hartkle, C. Bormann and B. Frank, "Constrained Application Protocol (CoAP)", Internet Draft, Nov. 2011.

[12] TrustChip Mobile Device Security; http://www.koolspan.com/trustchip/.

Authentication and certificate revocation in VANET

Carlos Gañán, Jorge Mata-Díaz, Oscar Esparza
Universitat Politècnica de Catalunya (UPC)
{carlos.ganan,jorge.mata,oscar.esparza}@entel.upc.edu

1. Background and Motivation of VANET authentication security

In the last years, wireless communications between vehicles have attracted extensive attention for their promise to contribute to a safer, more efficient, and more comfortable driving experience in the foreseeable future. This type of communications has induced the emergence of Vehicular ad hoc networks (VANETs), which consist of mobile nodes capable of communicating with each other (i.e. Vehicle to Vehicle Communication -V2V communication) and with infrastructure (i.e. Vehicle to Infrastructure Communication -V2I communication). To make these communications feasible, vehicles are equipped with *On-Board Units* (OBUs), and fixed communication units called *Road Side Units* (RSUs) are placed along the road. However, the open-medium nature of these networks makes it necessary to integrate in VANET security mechanisms such as authentication, message integrity, non-repudiation, confidentiality and privacy Authentication is considered the core security requirement for all networks, and VANETs are not an exception. The basic solution envisioned to provide authentication is to use digital certificates linked to a user by a Certification Authority (CA) [**Error! Reference source not found.**]. According to the IEEE 1609.2 standard [**Error! Reference source not found.**], vehicular networks will rely on the Public Key Infrastructure (PKI). In PKI, Certification Authorities (CA) issue digital certificates to network nodes. These certificates will be used by other nodes to verify the authenticity and integrity of messages. An efficient certificate management is crucial for the robust and reliable operation of any PKI.

2. Research Challenges/Problem statements

By default, each message in a VANET (especially safety ones) must include authenticated position information and a timestamp to avoid replay and tunnel attacks. The vehicle signs such messages with its private key, and it also includes its certificate to allow other users to verify its signature. Obviously, attaching a digital signature and a certificate to each message for the sake of security inevitably creates an overhead, which can be even larger than the message itself. Despite there are some ways of reducing this overhead, for instance data aggregation or the use of Elliptic Curve Cryptography (ECC) instead of RSA [**Error! Reference source not found.**], the overhead still is too high.

The provision of privacy to users is also a challenging problem. Instead of only one certificate, On Board Units (OBU) are equipped with a set of valid certificates (also called pseudonyms). Periodically, OBUs change the certificate they are using to avoid traceability and to assure some degree of anonymity. Eventually, OBUs will consume their certificate set, and they will need to update it. The classical PKI solution to update certificates involves the CA, which would send the new certificate set to the requesting OBU through the available Road Side Units (RSU). However, this centralized update approach may be impractical in large scale VANETs due to several reasons. For instance, the CA can become a bottleneck due to the number of update requests. Also, the update delay may be quite long, especially when compared to the short V2I communication duration between RSU and OBU.

Another challenge is the distribution of revocation data in the VANET. According to the IEEE 1609.2 standard [**Error! Reference source not found.**], VANETs will use Certificate Revocation Lists (CRLs) to distribute the status of certificates. Certificate Revocation Lists are needed for:

- Excluding compromised, faulty or illegitimate nodes,
- Preventing the use of compromised cryptographic material.

However, CRL pose a major problem: How to distribute large CRLs in a reasonable time with low

bandwidth utilization? Despite the simplicity of CRLs, their use in a vehicular network has two main drawbacks. CRLs in VANET are expected to be quite large because this type of network is expected to have many nodes (vehicles), and also because each vehicle may have many certificates (pseudonyms) that should be revoked once used. As a result, a VANET CRL might have a size of hundreds of Megabytes [**Error! Reference source not found.**-**Error! Reference source not found.**]. The distribution of such a huge structure within a VANET is a challenging issue and it has attracted the attention of many researchers [**Error! Reference source not found.**, **Error! Reference source not found.**, **Error! Reference source not found.**, **Error! Reference source not found.**]. The revocation scheme has to be able to obtain and check this CRL timely. Due to its probable huge size, the time elapsed to download and check a CRL can be a problem. Moreover, CRLs have also associated a problem of request implosion, i.e. vehicles may become synchronized around the CRL publication instant to request the newly issued CRL at or near the moment of publication. This burst of requests may cause network congestion that may introduce longer latency in the process of validating a certificate. The dependency on the infrastructure of the revocation service is also a problem to address. Most of the proposals require the presence of RSU to provide a reliable revocation service. However, in an early deployment of a VANET, the assumption of full coverage is not realistic. Designing a mechanism without any infrastructure support is still an open problem for consideration.

Revocation can also be achieved by relying on short-lived certificates which are automatically revoked after its lifetime expires. The problem is that, in VANETs, each vehicle takes life-critical actions based on the received messages from its neighboring vehicles (for instance, informing a car driver that an accident occurred). Hence, VANETs cannot solely depend on short-lived certificates, as a misbehaving vehicle can harm other vehicles until its certificate lifetime expires.

3. Proposed solutions, approaches, expert opinions and guidance

Regarding the revocation of digital certificates, proposals can be roughly classified as global or local depending on the extent of the revocation mechanism. *Local revocation approaches* propose mechanisms to enable a group of neighboring vehicles to revoke a nearby misbehaving node. They make possible revocation without the intervention of the infrastructure at the expense of trusting other vehicles criteria. On the other hand, *global revocation approaches* are based on the existence of a central entity, such as the CA, which is in charge of taking the revocation decision for a certain vehicle.

3.1. Global revocation approaches

Global revocation approaches assume the existence of a Trusted Third Party (TTP), which manages the revocation service. That is the case of the IEEE 1609.2 standard [**Error! Reference source not found.**], which proposes an architecture based on CAs. In this architecture each vehicle possesses several pseudonyms, which are publicized by means of short-lived certificates issued upon vehicle request. However, a revocation mechanism in VANET cannot rely uniquely on the use of short-lived certificates (e.g. as proposed in [**Error! Reference source not found.**]) because compromised or faulty vehicles could still endanger other nodes until the end of their certificate lifetimes. Thus, this standard also defines the format of the Certificate Revocation List (CRL) and assumes pervasive roadside architecture.

There are other global revocation approaches. For instance, Raya *et al.* [**Error! Reference source not found.**] have proposed the use of short-lived certificates that are preloaded in a tamper-proof device (TPD) or issued by an authorized provider or generated by the TPD and signed by the CA. Some authors [**Error! Reference source not found.**, **Error! Reference source not found.**], instead of using a single central authority, have proposed the use of regional certification authorities which must develop some trust relationships. Papadimitratos *et al.* [**Error! Reference source not found.**] suggest restricting the scope of the CRL within a region. Similarly, in [**Error! Reference source not found.**], each CA distributes the CRL to the RSUs in its domain through Ethernet. Then, the RSUs broadcast the new CRL to all the vehicles in that domain. In the case RSUs do not completely cover the domain of a CA, V2V communications are used to distribute the CRL to all the vehicles [**Error! Reference source not found.**]. This mechanism is also used

in [**Error! Reference source not found.**], where it is detailed a public key infrastructure mechanism based on bilinear mapping. In [**Error! Reference source not found.**] the authors present another adaptation of classic public key infrastructure to VANETS, but based on elliptic curves. Lin *et al.* in [**Error! Reference source not found.**] present another approach in which revocation is aided by the RSU. In this proposal, the CA sends CRLs to the roadside units. The RSUs then monitor the certificates in messages broadcasted by passing-by vehicles.

3.2. Local revocation approaches

Local revocation mechanisms deal with the revocation paradigm when there is no CA present in the network or it is not reachable. Without a central authority, no vehicle has the authority to decide when a node should be evicted from the VANET. Local revocation mechanisms often require that most nodes behave honestly to be able to detect attacks.

Some proposals in the literature divert from the IEEE 1609.2 standard and use online status checking protocols instead of CRLs to provide a revocation service in a decentralized manner. This is the case, of the Ad-hoc Distributed OCSP for Trust (ADOPT) [**Error! Reference source not found.**], which uses cached OCSP responses that are distributed and stored on intermediate nodes. The main drawback of this approach is that malicious or selfish nodes may subvert the system deciding not to respond to these queries.

Other proposals base the revocation service on detecting a vehicle to be misbehaving by a set of other vehicles. Then, the detecting set may cooperatively revoke the credential of the misbehaving node from their neighborhood. Moore *et al.* proposed in [**Error! Reference source not found.**] a revocation mechanism aiming to prevent an attacker from falsely voting against legitimate nodes. Raya *et al.* in [**Error! Reference source not found.**] proposed a mechanism to temporarily revoke an attacker if the CA is unavailable. To do so, the number of accusing neighbor users must exceed a threshold. A similar mechanism based also on vehicle voting is proposed in [**Error! Reference source not found.**]. Another proposal uses a game-theoretic revocation approach to define the best strategy for each individual vehicle [**Error! Reference source not found.**, **Error! Reference source not found.**].

3.3. Research Direction and trend

Current research is mainly focused on trying to provide a good trade-off between security and performance. Reliability of the revocation service should be provided, that is, that service should be available at all times, even if there is no coverage. However, this availability should not adversely affect too much to resources. The revocation service should consume as little resources as possible (CPU, memory, storage, bandwidth, etc.), because validation is often carried out in constrained environments.

Regarding the main trends in the research community, some proposals intend to decentralize the revocation service in order to eliminate the dependency of central authorities. These proposals take advantage of V2V communications to disseminate the revocation information. On the other hand, other more centralized approaches intend to reduce the overhead introduced by the issuance of huge CRLs. Several mechanisms have been proposed to deal with the dissemination of these CRLs. Some try to reduce the size of the CRL either using regional CAs [**Error! Reference source not found.**] or compressing the CRL by using probabilistic data structures. There exists other type of solutions that try to take advantage of coding techniques to improve the delivery of certificate status information. For instance in [**Error! Reference source not found.**], the authors take advantage of digital fountain codes to avoid additional retransmissions.

4. Conclusions

To provide assurance that messages are reliable, certificate revocation procedures must be enacted to prevent messages sent by malicious users and malfunctioning equipment from being accepted by members of the VANET. The current IEEE 1609.2 security standard is considered by many to be both slow and insufficient in meeting the needs of VANET authentication security. Several works discussed have

developed alternative methods, while still utilizing the security backbone set in place by the standard. Others attacked the problem from a completely different approach. However, there still exists a list of open problems that can be further investigated under the context of authentication. VANET authentication is still an active area of research and more research is needed to address the challenges before VANETs can be deployed on the roads effectively and efficiently.

References

[1] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *Telecommunications, 2007. ITST '07. 7th International Conference on ITS*, Jun. 2007, pp. 1 –6.

[2] "IEEE trial-use standard for wireless access in vehicular environments - security services for applications and management messages," *IEEE Std 1609.2-2006*, pp. 1–105, 2006.

[3] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, ser. SASN '05, 2005, pp. 11–21.

[4] M. Nowatkowski, C. McManus, J. Wolfgang, and H. Owen, "Cooperative certificate revocation list distribution methods in vanets," in *Ad Hoc Networks*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. plus 0.5em minus 0.4emSpringer Berlin Heidelberg, 2010, vol. 28, pp. 652–665.

[5] J. Haas, Y.-C. Hu, and K. Laberteaux, "Efficient certificate revocation list organization and distribution," *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 3, pp. 595 –604, march 2011.

[6] A. Wasef and X. Shen, "MAAC: Message authentication acceleration protocol for vehicular ad hoc networks," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 30 2009-dec. 4 2009, pp. 1 –6.

[7] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: design and architecture," *Communications Magazine, IEEE*, vol. 46, no. 11, pp. 100 –109, Nov. 2008.

[8] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, "Security certificate revocation list distribution for vanet," in *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, ser. VANET '08, 2008, pp. 88–89.

[9] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems," in *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*, ser. VANET '08, 2008, pp. 86–87.

[10] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, Apr. 2008, pp. 1229 –1237.

[11] A. Wasef, Y. Jiang, and X. Shen, "DCS: An Efficient Distributed-Certificate-Service Scheme for Vehicular Networks," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 2, pp. 533 –549, feb. 2010.

[12] C.-I. Fan, R.-H. Hsu, and C.-H. Tseng, "Pairing-based message authentication scheme with privacy protection in vehicular ad hoc networks," in *Proceedings of the International Conference on Mobile Technology, Applications, and Systems*, ser. Mobility '08, 2008, pp. 82:1–82:7.

[13] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, "Cross-layer privacy enhancement and non-repudiation in vehicular communication," in *4th Workshop on Mobile Ad-Hoc Networks (WMAN'07)*, 2007.

[14] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 88 –95, Apr. 2008.

[15] G. F. Marias, K. Papapanagiotou, and P. Georgiadis, "ADOPT. a distributed ocsp for trust establishment in manets," *11th European Wireless Conference 2005*.

[16] T. Moore, J. Clulow, S. Nagaraja, and R. Anderson, "New strategies for revocation in ad-hoc networks," in *Proceedings of the 4th European conference on Security and privacy in ad-hoc and sensor networks*, ser. ESAS'07, 2007, pp. 232–246.

[17] A. Wasef and X. Shen, "EDR: Efficient Decentralized Revocation Protocol for Vehicular Ad Hoc Networks," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 9, pp. 5214 –5224, nov. 2009.

[18] M. Raya, M. H. Manshaei, M. Félegyhazi, and J.-P. Hubaux, "Revocation games in ephemeral networks," in *Proceedings of the 15th ACM conference on Computer and communications security*, ser. CCS '08, 2008, pp. 199–210.

[19] I. Bilogrevic, M. Manshaei, M. Raya, and J.-P. Hubaux, "Optimal Revocations in Ephemeral Networks: A Game-Theoretic Framework," in *Proceedings of the 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt 2010)*. plus 0.5em minus 0.4emIEEE, 2010, pp. 184–193.

IDS Countermeasures to Protect QoS of 6LoWPAN from Internal Threats

Jonathan Loo and AnhTuan Lee
Department of Computer Communication, School of Engineering and Information Sciences,
Middlesex University (MDX), UK
{j.loo, a.lee}@mdx.ac.uk

1. Background and Motivation

The Internet of Things (IoT) concepts are currently attracting an extensive interest due to its promising applications in a wide range of applications, from transportation and logistics, health care, smart environment, to personal and social, gaming, robot, city information [1]. Fueling to bring IoT concept to real life, IEFT is working on 6LoWPAN, which is a standard to integrate IPv6 with the IEEE 802.15.4 based Low-power and Lossy Wireless Personal Area Network (LoWPAN), also referred to as Wireless Sensor Networks (WSN). This standard allows the use of existing IP network infrastructure and the huge address space of IPv6; ideally, vast number of smart objects can be deployed in local WSNs which be used to harvest enormous data and information through the Internet. Many applications of 6LoWPAN strictly require the information security and robustness Quality of Services, so its security issues need to be considered carefully. Cryptography techniques are applied as the front line defense as in many other networks. However, in this context, adversaries can easily tamper the WSN devices to obtain the network encryption keys and change their operation code. The consequence is that these compromised nodes are utilised to manipulate, abuse, or bring down the network QoS. These so-called internal threats are difficult to be detected because under the view of the cryptography line, all nodes are still authenticated and legitimate. Intrusion Detection System (IDS) is one of the potential candidates that needs to be added to the security system to deal with such attacks.

2. Problem Statements

One of the challenges is to assess 6LoWPAN threats to weigh their impact on network performance and study theit behaviours for further protection. The characteristics of network devices (low power, limited energy) and communication (low power and lossy, frequently topology change) expose 6LoWPAN to many threats. While some of them could be found in wireless sensor or ad-hoc network context, others are specific to 6LoWPAN. In general, threats toward 6LoWPAN may come from all of its sides: the Internet, adaptation layer or its sensor side.

- The Internet side raises the threats of authenticating between users and sensor motes, sensor network availability, or user accountability. For example, the adversaries can access the information illegally, eavesdrop sensitive information or assessing the network using user accountability.
- 6LoWPAN adaptation layer can be vulnerable from the fragmentation attacks which can make the node run out of resource [7].
- Threats from the sensor side: due to the weak secure nature of devices and wireless environment, those threats are spread to all of its layers, from jamming at physical transmission; exhaustion attack at the data link; dropping packets at the network layer; to DoS to the transport and application layer.

Among those attacks, internal threats towards sensor network layer are feasible and create significant impact to network QoS which prevent the real-time applications and services.

IDS techniques are commonly applied to this context to deal with such threats. The most common IDS approaches are misuse, anomaly-based and specification-based. A misuse IDS is based on patterns of the known attacks and need to store large data so that it is not favoured in 6LoWPAN because the knowledge of the attacks is not well-studied while the security resource is constrained. The anomaly-based IDS focus on monitoring the deviation between normal and anomaly network performance, while specification-based IDS

focus on profiling the network behaviours. Each of these approaches has its own advantages; however, using them alone cannot solve the internal threats properly. For example, for anomaly-based IDS, in case of topology attacks, the compromised nodes can form a bad topology while still performs normal like the legitimate nodes. This may lead to QoS degradation; however, the anomaly-based alone cannot detect this type of threats because they only look at the node performance. On the other hand, specification-based IDS normally assure behaviours of the protocol but lack of considering to the node performances, which will lead to similar undetectable QoS attack scenarios. One challenge is to combine these two methods to have a robust security system while saving resources by their cooperation.

3. Approaches, expert opinions and guidance

There has been a wide-range of techniques applied in anomaly-based IDS. One of the focuses is to set up the threshold of the performance deviation. Lee et al. [2] calculate the threshold in clustering WSN by using the number of cluster nodes, the value of the key dissemination limit, and the distance from the base station to each cluster. This method adapts the topology changes due to the moving of the nodes. Sang and Tae [3] used other four factors: the node energy level, neighbour nodes list, message transmission rate and error rate in the transmission to calculate a dynamic threshold for detecting DoS attacks. Parekh and Cam [4] used a Directed Acyclic Graph and Probability table to represent the dynamic site condition to calculate the threshold value.

Artificial Intelligent techniques can also be applied to optimise the objective of the solution. Rong et al. [5] defined a simple payoff matrix with probability measures for the IDS to protect important nodes in the network effectively from the DoS attack. Estiri [6] proposed a repeated game model for detecting the dropping packet attacks which reward the node reputation every time it forwards and cooperates, while punishing every time it does not. Banerjee, S., et al. [7] combines the Emotional Ants and the conventional machine learning for keeping track of the intruder trials. The IDS agent works as the ant agent and later is transformed to be the emotional ant agent for making decision.

The differentiate between legitimate and malicious behaviours is also studied through statistical models. Phuong et al. [8] used the Cumulative Sum to detect changes based on the cumulative effect of the changes made in the random sequence. Ponomarchuk [9] analysed the number of received packets in a time window of a given length and inter-arrival time of packets for detecting anomaly behaviours. The packet Reception Rate was calculated based on the binomial distribution while the inter-arrival time was based on the exponential distribution. David et al. [10] used Bayesian Trust Model for calculating the MAC sub-layer data of WSN to mitigate the unfairness and consequent upon the DoS attacks.

The feature subset on the collected data is classified by the Data Mining approach. Kaplantis et al. [11] used Support Vector Machine with polynomial kernel or Radial Basis Function (RBF) model for detecting selective forwarding and black hole attacks. The chosen parameters for monitoring are bandwidth and hop count within a sliding window.

On the other hand, specification-based approach can fit well with the principles of abstraction, simplify the feature selection and tailor the monitor to the needs of their own systems. This approach can scale well and simplifies the test operation for deciding whether or not a set of events constitutes a violation. It can also take advantage of the knowledge system administrators have about possible attacks. The main techniques used for these specifications are state machine transitions, machine learning for pattern recognition and statistical analysis to derive automatically the program specifications [12, 13]. Literature on ad hoc and wireless sensor network security presented some specification-based IDS on several protocols such as AODV [14], OLSR [15] and CoP [16].

4. Research direction

The combination of anomaly-based and specification-based approach should be considered to take advantages of both approaches' strength and minimise their weakness. The potential system that we envisage

has three main parts (i) a specification-based module that profile the network behaviours through its underlying routing protocol – the Routing Protocol for Low power and lossy network (RPL) (ii) the anomaly-based module that co-operated with specification-based to monitor the node performance, and (iii) the statistical-based component to reveal the attacker source. These modules work in cooperation, which means the results of one module can be reused for the other to minimise the security expense. The system model is presented in Figure 1.

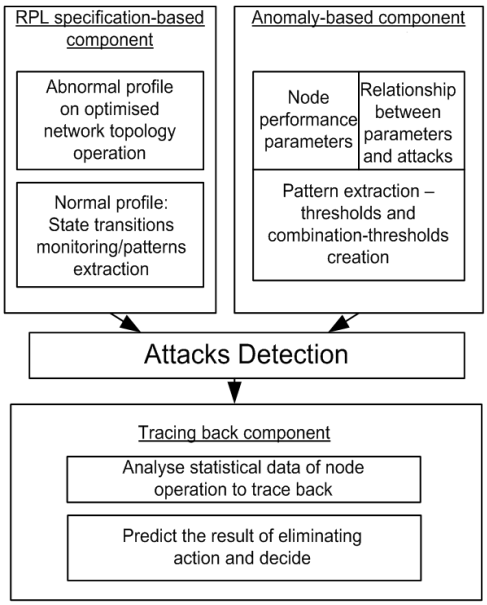

Figure 1. Combination of Specification-based and Anomaly-based IDS

The brief functions of each module are:

- **RPL Specification-based IDS component:** to monitor and extract the topology information, for example, the parent-child relationship, or topology change frequency to detect any invalid or unstable in the topology.
- **Anomaly-based IDS component:** to analyse the relationships of some network performance parameters in the event of attacks as symptoms or evidences to diagnose the attacks. We focus on the technique that detects based on the combination of those evidences, by building the relationship model between them using statistical and probability technique, rather than decide based on single type of evidences alone.
- **Tracing back component:** this module benefits from the analysis results of the two IDS modules to predict the malicious node locations and decide further actions.

Our idea can be illustrated in Figure 2, in which we use two cooperated layers IDS to provide the detection ability for as many attacks as possible. After detecting the malicious behaviors, the system will attempt to trace back and eliminate the attacker node, to ensure the network QoS.

A system like that can be built with many options: from the architectures, the features to extract for monitoring, or the detection techniques. The crucial mission is to choose the most effective solution while satisfying the network resource saving requirements.

The internal threats for 6LoWPAN QoS should be assessed thoroughly and put into the network operation to evaluate the effectiveness of the defending system. Other design parameters such as the distribution of IDS agents, feature selections and resource saving will be evaluated through simulations.

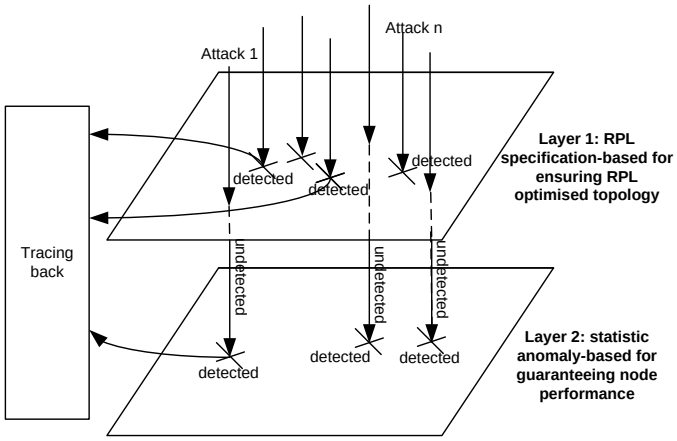

Figure 2. IDS protection layers for securing 6LoWPAN from internal QoS threats

5. Conclusion

6LoWPAN plays an important role in bring the IoT concept to real life to benefit from its extensive range of modern applications. Securing its QoS is crucial and mandatory due to the customer requirements in many real-time services. Cryptography techniques applied as the front line of defence or deterrent can easily be broken due to the weak secure nature of LoWPAN devices and wireless environment. Compromised nodes could lead to insider attacks without being detected by any cryptography and create severe impact in network QoS. IDS is the main approach for such a problem, especially when dealing with the feasible internal threats in 6LoWPAN. A potential research direction is to combine the most two effective IDS approaches – the specification-based and anomaly-based to benefit from their advantages while minise the limitations. In that direction, the specification-based module should provide a fast and accurate way to examine the optimisation of the typology, while the anomaly-based module should pay attention to the node behaviours. The cooperation of these two modules would guarantee the standard for network QoS, and optimise the resource spent for security missions, while provide further ability to trace back the malicious resource, which is vital for securing 6LoWPAN.

Reference

[1] Atzori, L., A. Iera, and G. Morabito, *The Internet of Things: A survey.* Comput. Netw., 2010. **54**(15): p. 2787-2805.

[2] Lee, S.J., H.Y. Lee, and T.H. Cho, *A Threshold Determining Method for the Dynamic Filtering in Wireless Sensor Networks Based on Fuzzy Logic.* IJCSNS International Journal of Computer Science and Network Security, 2008. **8**(4).

[3] Chi, S.H. and T.H. Cho, *Fuzzy Logic Anomaly Detection Scheme for Directed Diffusion Based Sensor Networks*, in *FSKD 2006*2006. p. 725-734.

[4] Parekh, B. and H. Cam, *Minimizing False Alarms on Intrusion Detection for Wireless Sensor Networks in Realistic Environments*, in *Military Communications Conference*2007.

[5] Dong, R., et al., *Intrusion Detection System Based on Payoff Matrix for Wireless Sensor Networks*, in *Genetic and Evolutionary Computing*2009.

[6] Estiri, M. and A. Khademzadeh, *A game-theoretical model for intrusion detection in wireless sensor networks*, in *Electrical and Computer Engineering (CCECE), 2010 23rd Canadian Conference*2010 Calgary, AB p. 1-5.

[7] Banerjee, S., et al., *Intrusion detection on sensor networks using emotional ants.* International Journal of Applied Science and Computations, 2005. **12**(3): p. 152-173.

[8] Phuong, T.V., et al., *An Anomaly Detection Algorithm for Detecting Attacks in Wireless Sensor Networks*. Intelligence and Security Informatics. Vol. Lecture Notes in Computer Science, 2006, Volume 3975/2006. 2006: Springer.

[9] Ponomarchuk, Y. and D.-W. Seo, *Intrusion detection based on traffic analysis in wireless sensor networks*, in *Wireless and Optical Communications Conference (WOCC), 2010 19th Annual*2010 Shanghai p. 1 - 7

[10] David, B.M. and R.T.d.S. Jr, *A Bayesian Trust Model for the MAC Layer in IEEE 802.15.4 Networks*, in *I2TS 2010 - 9th International Information and Telecommunication Technologies Symposium*2010.

[11] Kaplantzis, S., et al., *Detecting Selective Forwarding Attacks in Wireless Sensor Networks using Support Vector Machines*, in *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference*2007: Melbourne, Qld. . p. 335 - 340

[12] Sekar, R., et al., *Specification-based anomaly detection: a new approach for detecting network intrusions*, in *Proceedings of the 9th ACM conference on Computer and communications security*2002, ACM: Washington, DC, USA. p. 265-274.

[13] Stakhanova, N., S. Basu, and J. Wong, *On the symbiosis of specification-based and anomaly-based detection*, in *Computers & security 29 (2010)*2010. p. 253 – 268.

[14] Ning, P. and K. Sun, *How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-Hoc Routing Protocols*, in *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society* 2003. p. 60-67.

[15] Tseng, C.H., et al., *A Specification-Based Intrusion Detection Model for OLSR*, in *Recent Advance in Intrusion Detection RAID 2005*2005. p. 330-350.

[16] Orset, J.-M., B. Alcalde, and A. Cavalli, *An EFSM-Based Intrusion Detection System for Ad Hoc Networks*, in *Lecture Notes in Computer Science, Volume 3707/2005*, Springer, Editor 2005. p. 400-413.

Lightweight Intrusion Detection Systems for Wireless Ad-hoc / Sensor Networks

Christiana Ioannou and Vasos Vassiliou
Department of Computer Science
University of Cyprus
Nicosia, Cyprus
{cioannou, vasosv}@cs.ucy.ac.cy

1. Motivation and Background

Wireless Sensor Networks (WSN) are popular for their adaptive architecture, which enables them to run a number of applications, most notably monitoring and surveillance. However, sensor nodes have hardware limitations, which prevent them from utilizing complex security methods to establish a secure network. Intrusion Detection Security Systems (IDS) have long been proposed for wired and wireless sensor networks, to detect and prevent entrance and propagation of malicious attacks. The power, energy, and memory constraints of sensor nodes make it harder to apply IDS algorithms that have been proposed for wired and wireless networks in the WSN domain.

2. Research Challenges or Problem Statements

Wireless Sensor Networks (WSNs) have received increasing attention from researches and industry for their ability to provide low-cost, low-power, and multifunctional networks. Some of the applications of WSNs can be found in environmental and medical monitoring, military operations, and space exploration. The main characteristics that distinguish WSNs from other wireless networks are (a) a random and dense deployment (b) self-organization and cooperative effort of sensor nodes, (c) frequently changing topology due to wireless channel fading and node failures, (d) limitations in energy, transmit power, memory and computing power and (e) difficulty in enforcing demanding security solutions.

One challenge that all computer networks have in common is the establishment of a security system in the network. Precautions to prevent malicious code and methods for reversing the malicious effects were developed to help users in wired and wireless networks. However, existing methods usually fail in identifying unknown malicious attacks and require significant memory and processing capacity, which are a limited resource for WSNs. It is our belief that a light-weight intrusion detection system (IDS) that imitates the human immune system and uses anomaly detection will be able to detect and prevent novel attacks in sensor networks.

The aim of the human immune system is to prevent, detect, and act upon a non-self entity in the human body. The human immune system is mainly characterized by its ability to distinguish a self cell from a non-self cell, has multi-layer and distributed defenses, it is unique per human, and it acquires knowledge from novel viruses which is used to create antibodies and inform the rest of the human body The analogy between the human immune system and computer and network security has long been proposed and adapted in establishing secure systems.

An IDS system has two main detection algorithms (a) pattern (also known as misuse) detection and (b) anomaly detection. Pattern detection bases its detection algorithms on existing knowledge. Patterns or signatures of known attacks are stored in a database and are used to compare with current activity. When there is match between the current activity's signature and one of the attacks, then a malicious program is detected and an alarm is raised. The advantage of using pattern detection is that it has low false alarm rates. The disadvantage is that it requires memory space to save its knowledge. Unlike anomaly detection, misuse detection is used to detect only known attacks.

However, anomaly detection requires constant monitoring network traffic, and computation time for extracting parameters and constructing the behavior pattern. At the same time, distribution of IDS agents

within a WSN can also impose more overhead to the WSN. One challenge is to determine the overheads impose and what will constitute a "lightweight" IDS system.

3. Research Direction and Trends

3.1. Human Immune System

Many research groups concentrate on the analogy of biological system methods for survival with routing and self-organization algorithms to provide security on the Internet. The human immune system survival mode has been proven to be untouchable for the longest period known to human. It has achieved that by bearing certain characteristics. Applying the detection and action characteristics of the human immune system to the WSN may result to the same effectiveness. Some characteristics of the human immune system are knowledge of one's self entities, imperfect competition and memory. Equipped with benign network and sensor behavior, it can create detect any non-self activity within the sensor itself or the network. The human immune system remembers previous attacks and responds fairly quickly. In the case of novel attacks, it takes more time to defend itself, but it is still able to respond [11]. The same characteristics should be used in the security systems. The detector should be able to identify known and new attacks. Misuse detection algorithms used in IDSs are able to detect known attacks [12], while anomaly detection algorithms are used to detect novel attacks. Imperfect detection, and it has two phases, the learning phase and the distributed detection phase. The human immune system learns from the first response of the disease and then that learning is distributed in the individual or human population [11]. Imperfect detection is called a misuse-detection system in the computer security world [10]. To be effective, WSN systems should establish the same technique. Cooperative effort through the network such as collaboration of local and global agents would succeed in confining the attack at a small section in the network [13]. Silva et al., in **Error! Reference source not found.**, propose using monitoring nodes in the network that will be responsible for a cluster of sensor nodes. Bhuse and Gupta, in [9], propose Triangulation, in which each sensor node monitors traffic within its range and notifies other sensor nodes when it encounters an intruder.

3.2. Intrusion Detection Systems

Intrusion detection systems using anomaly detection at real-time have long been proposed to provide a secure system that can detect a wide range of security violations [8][2]. The main motivation of the IDS was to overcome security flaws from existing systems and prevent misuse of information by insiders that take advantage of their privileges. IDSs were also proposed for Wireless Sensor Networks, in which they aim in to provide security while at the same time take into consideration the limitations of WSNs. The main limitation of WSNs, which distinguishes them from other wireless networks, is the limitations on energy, transmitting power, memory and computing power [5].

The anomaly detection method uses user profiles to detect new attacks. Any deviation from what is the normal profile is classified as potential attack. Detecting new attacks at an early stage can avoid any damages that the intruder may cause. However, anomaly detection can create false positive and false negative alarms. A false positive alarm is caused when new benign behavior is classified as malicious [10]. False positive alarms are a result of creating a too specific normal profile. The advantage of defining a specific normal profile is that the false negative rate is small relative to a more general definition of what is normal activity. The disadvantage is that it will require resources such as memory, computation resources and time to save the normal behavior profile and compare activity detected with what is normal activity [1][6]. On the other hand, a more generally defined normal behavior profile, which requires fewer resources, may cause false negatives. False negative alarms are caused when the security system fails to identify a malicious attack [7].

Current research focuses in targeting specific attacks at specific network layers [4][8][9][6][3]. Upon detecting a malicious node, the proposed algorithms, redirect traffic to avoid the malicious node. Taking into consideration the findings of previous work, a more complete target attack group will be wider by evaluating data from all network layers.

4. Proposed solutions, approaches, expert opinions and guidance

We propose the construction of an IDS that correlates the operations of the human immune system in sensor networks. To achieve a lightweight IDS, we must first identify self and non-self-behavior by considering specific types of application, operating systems and communication platforms (creating uniqueness). Once we define normal profile we will create models that can be used to detect malicious intent (distinguishing self from non-self). The third step is to deploy our IDS architecture and calibrate it to new findings and according to the false alarm rate and the fourth step is to distribute this activity and enable multiple level defenses to emerge.

The IDS´ tasks are to (a) detect, (b) prevent, (c) update its intrusion model with possible attack, and (d) inform the rest of the network for the intrusion. At the deployment stage, IDS will be calibrated to capture novel attacks. Experimental parameters such as identifying the boundaries of what is considered normal behavior, distribution of IDS agents, monitoring intervals, and false alarm rates will be evaluated per application demands and WSN capabilities.

5. Conclusion

WNS have received increased attention for their capability to provide low-cost, low-power, and multifunctional networks. Some of the applications of WSNs can be found in environment, medical monitoring, military purposes, and space exploration. Establishing security measures in WSN is both mandatory and challenging. IDS using anomaly detection is a lightweight security technique that can detect malicious intervention within WSN. It is evident that human immune characteristics can be used as guidelines for establishing a secure WSN system. We propose an IDS that uses human immune system characteristics as a blueprint for constructing the IDS architecture. Cross-layer data can provide insights for all network attacks whereas proposed work used information from one or two network layers thus targeting a specific group of attacks. WSNs ‘establishment is the prime factor for determining the detection timing and distribution methods. The objective to establish a secure IDS is to be able to guarantee data integrity, sensor network availability, and confidentiality with minimal operational cost.

References

[1] C. Karlof, N. Sastry, and D. Wagner. “TinySec: A Link Layer Security Architecture for Wireless Sensor Networks,” Proceedings of the 2nd International conference on Embedded network systems, pp.162-175, 2004

[2] D. E. Denning, “An Intrusion-Detection Model,” *IEEE Trans. Softw. Eng, vol.* 13, pp. 222-232 , February 1987.

[3] K. Ioannis, T. Dimitriou, and F. C. Freiling, "Towards intrusion detection in wireless sensor networks," In Proc. of the 13th European Wireless Conference, 2007.

[4] M. Drozda, S. Schaust, and H. Szczerbicka, “AIS for Misbehavior Detection in Wireless Sensor Networks: Performance and Design Principles”, in Proc. of IEEE Congress on Evolutionary Computation, 2007.

[5] M. Ilyas and I. Mahgoub. “Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems,” CRC Press, 2005

[6] R. Muraleedharan and L. A. Osadciw, “Cross Layer Security Protocol Using Swarm Intelligence in WSN Applications,” 2007 IEEE Long Island Systems, Applications, and Technology Conference (LISAT2007) Farmingdale, New York, May 2007.

[7] S. Northcutt, L. Zeltser, S. Winters, K. K. Frederick, R. W. Ritchey. “Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems,” New Riders, First Edition, July 2003

[8] S. Schaust and H. Szczerbicka. “Misbehaviour Detection for Wireless Sensor Networks- Necessary or Not?”, *Proc. of the 6. Fachgespräch "Drahtlose Sensornetze" der GI/ITG-Fachgruppe "Kommunikation und Verteilte Systeme"*, pp. 51-54, Aachen, Germany, 2007

[9] V. Bhuse, and A. Gupta, Anomaly Intrusion Detection in Wireless Sensor Networks, *J. High Speed Networks, Vol. 15, No. 1, pp. 33-51,* 2006.

[10] W. Lee and D. Xiang, “Information-Theoretic Measures for Anomaly Detection,” IEEE Symposium on Security and Privacy, 2001

[11] S. Forrest, S.A. Hofmeyr, and A. Somayaji, “Computer Immunology,” *Communications of the ACM*. Vol. 40, No 10, pp. 88-96, October 1997

[12] Adware. (2006, January). Available: http://www.lavasoft.com/software/adware.

[13] R. Roman, J. Zhou and J. Lopez, “Applying Intrusion Detection Systems to Wireless Sensor Networks”, *Proc. of the 3rd IEEE Consumer Communications and Networking Conference (CCNC 2006), Vol.* 1, pp. 640- 644, *Jan. 2006*

Lightweight security and privacy protocols formalization and reference architectures for Wireless Networked Moving Objects (WiNeMO)

Denis Trček
University of Ljubljana, Slovenia
denis.trcek@guest.arnes.si

1. Background / Motivation

Pervasive computing (also referred to as ubiquitous computing) is an emerging paradigm, where, as opposed to traditional computer networks built around mainframes, desktops and laptops, these networks are being intensively extended by devices with limited computational resources, typically RFIDs (radio frequency identification systems), sensors and actuators.

What is important fact here is that such devices are supposed to outgrow all other kinds of networked devices in the global internet, thus leading us towards so called Internet of Things, or IoT (according to Gartner Group RFID's market share is supposed to reach 3.5 billion U.S. dollars already this year [1], and taking into account the "fifty cents limit" for RFIDs this would imply a comparable order of magnitude of deployed RFID "sensors").

Now taking into account that these are primitive computational devices with also limited power / energy resources, the need for so called lightweight security (and privacy) solutions, and protocols in particular, becomes evident. Not only from a pure market driven point of view, but also from legislative point of view where bodies like the EU are pressing RFID (and other IoT) developers and producers to consider privacy issues [2, 3].

2. Research challenges / Problem statements

The most evident challenges with WiNeMO systems as to security and privacy through "lightweightness perpective"are the following ones:

- These systems have notable limitations related to energy / power consumption, because they have (in principle) weak autonomy or are even passively powered.
- Similarly, these systems have notable limitations due to often imposed physical dimensions.
- Finally, many of these systems are all-in-silicon devices. This holds true not only for RFIDs, but also other ASIC (Application Specific Integrated Circuits) devices. Therefore technological limits as such come into play (the number of logical gates of this and that type, etc.).

Clearly, the above issues are interrelated: the number of gates influences power consumption, while this number itself is affected by physical dimensions, etc. Nevertheless, these issues are not about "total correlation" and can (and should be) treated as stated.

Now the next logical question arises:

- If these are the imposed limitations, we need security (and privacy) solutions (i.e. protocols) that are efficient as much as possible. Put another way – we need lightweight security and privacy protocols. Now what does this exactly mean? How to define what lightweight protocol means?
- Further, these devices may be deployed within other devices that are not subject to such stringent limitations, e.g., RFIDs and sensors may be built into mobile terminals like smart-phones. The next two questions are: How much in such cases lightweight protocol issues still matter? Where to draw the borderline between such sensors deploying terminals where lightweight issues matter and where these issues can be neglected?

Getting to the first basic question – what actually is lightweight protocol? How to formally define it?

Having a short survey of scientific papers at Elsevier's ScienceDirect and IEEE Xplore, and searching for related key-words, one can obtain the following results that are given in the below table (number of hits are given in columns 2 and 3, while the first column contains search terms):

	Elsevier ScienceDirect	IEEE Xplore
lightweight protocol	6834	1137
lightweight protocol definition	2907	9
lightweight protocol quantification	441	1323
lightweight protocol formalization	127	2

Surprisingly, the above search results in numerous lightweight protocols, so literally thousands of such protocols already exist. However, analyzing abstracts of the above results for the last three search strings, one finds out that a general, exact, formal, and technology focused definition of lightweight protocol is still needed.

One example of formalization can be found in [4]. This attempt is fine as long as all-in-silicon devices (e.g., RFIDs) are considered. However, even for these devices the radio part is still briefly addressed, not to mention specifics when other ASIC solutions are considered. Further, an example of lightweight protocols that are aligned with above formalization can be found in [5].

3. Proposed solutions, approaches, expert opinions and guidance:

To find solutions to the so far identified challenges, the following steps (approaches) are proposed to be taken:

- Explicit agreement on (and a formal definition) of what lightweight protocol actually means / is. Put another way, metrics is needed that provides means to measure "lighweightness". Can be this metric expressible in, e.g., number of NAND gates that are deployed for realization of a security protocol?
- Various deployment technologies will have to be considered and included, and one most likely distinction will be made between IoT entities that directly care for their communication needs as it is the case with all-in-silicon devices (like RFIDs), and between IoT entities that take only minimal communications efforts, and the rest is done on their behalf by a microprocessor or microcontroller (like this is the case with, e.g., smart-phones). Put another way, as IoT entities have to communicate at least at the most primitive level, we have to decide, which level this will be, e.g., Inter-Integrated Circuit, I^2C [6] or Serial Peripheral Interface SPI, [7], or higher level specification like IEEE 802.12.4 [8], 6LoWPAN [9], or some new abstract specification? Therefore what kind of granulation is to be considered?
- Practical guidelines on how to build lightweight protocols for certain contexts. Maybe this can be achieved by appropriate number of so called reference architectures? So if a certain protocol fits into appropriate model (computational architecture) than it can be considered (and also implemented in reality) as lightweight for such and such environment and purpose.

To make efforts sensible, involvement of experts from industry and standardization bodies would be needed. Further, these protocols, especially those providing privacy, will be strongly influenced by legislation. Therefore these protocols will not be "machine-sufficient", but will require some minimal intervention from users, which brings a new dimension to low-level protocol designing process. Therefore this is another important research and implementation issue:

- If various modes are to be supported due to privacy considerations, how to efficiently enable such a low-level interaction from a user in a lightweight manner?

4. Conclusions

The internet is rapidly expanding by so called Internet of Things, IoT, which includes RFIDs, sensors and actuators. These devices are just about to outgrow all other devices connected to the global internet.

However, these devices have many specifics, especially in terms of available computing power and energy / power consumption, but also stringent production costs are often present in this domain. By being so widely deployed on one side, and so limited in capabilities on the other, the basic problem is how to provide privacy and security for these ubiquitous entities in an efficient, "lightweight manner". This area, despite its importance, still lacks some important formal definitions, and architectural and technological guidance, together with corresponding standardization efforts.

5. References

[1] Wyld, D., Believe The Hype of RFID, Bukisa, http://www.bukisa.com/articles/372766_believe-the-hype-of-rfid, last accessed on April 12, 2012.

[2] e-practice.eu, Commission launches consultation on radio frequency identification (RFID), March 3, 2008, European Communities, http://www.epractice.eu/document/4426.

[3] European Commission, Privacy and electronic communications directive, 02/58/EC, Official Journal of the European Communities, L201, Brussels, 2002.

[4] Trček D., Kovač D., Formal apparatus for measurement of lightweight protocols, Computer Standards and Interfaces, 31(2), 305–308, Elsevier, 2008, http://dx.doi.org/10.1016/j.csi.2008.02.004.

[5] Trček D., Japinnen P., RFID security, Eds. Zhang Y., Tianruo L., Chen J., RFID and sensor networks : architectures, protocols, security, and integrations, pp. 147-168, Taylor & Francis, 2010.

[6] Philips, THE I 2C-BUS SPECIFICATION, v 2.1, 2000, http://www.nxp.com/acrobat_download/literature/9398/39340011.pdf.

[7] Motorola, SPI Block Guide, V 3.06, 2003, http://www.ee.nmt.edu/~teare/ee308l/datasheets/S12SPIV3.pdf.

[8] IEEE, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Data Rate Wireless Personal Area Networks (WPAN), IEEE Standard 802.15.4, IEEE: Piscataway, 2006.

[9] Rodrigues, J.J.P.C., Neves, P.A.C.S, A survey on IP-based wireless sensor network solutions, Int. J. Commun. Syst. 2010, 23, pp. 963-998.