Trust-based Security in Wireless Sensor Networks using Game Theory

Kavitha B M
Department of computer science and Engg.
Akshya Institute of Technology
Tumkur, India

Mr. Harish H K
Department of computer science and Engg.
Akshya Institute of Technology
Tumkur, India

***Abstract* — at current, Sensor Networks and the emerging Internet of Things standard are playing a key role in the industry and in academic research. Internet of Things (IoT) is an included part of Future Internet and could be distinct as a dynamic global network infrastructure with self configuring capabilities based on typical and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and employ intelligent interfaces, and are seamlessly integrated into the information network. In this paper we presented the overview of internet of thing, security and challenges for Internet of Things (IoT), we also proposed features of Intenet of thing in this paper.**

Keywords-; Energy awareness, game theory, Internet of Things (IoT), security, trust evaluation,

I. INTRODUCTION

In the future Internet of Things (IoT), the everyday objects which contain us will become positive actors of the Internet, generating and consuming information. The elements of the IoT comprise not only those devices that are already deeply rooted in the technological world (such as cars or fridges), but also objects foreign to this environment (garments or perishable food), or even living beings (plantations, forest or livestock). By embedding computational capabilities in all kinds of objects and living beings, it will be possible to present a qualitative and quantitative leap in several sectors: healthcare, logistics, domotics, entertainment, and so on. In fact, one of the most important elements in the IoT paradigm is wireless sensor networks (WSN). The benefits of concerning both WSN and other IoT elements go beyond remote access, as heterogeneous information systems can be able to collaborate and present general services. This integration is not simple speculation, but a truth supported by several international companies. Noteworthy examples are „A Smarter Planet" [1], a strategy developed by IBM which deems sensors as basic pillars in intelligent water management systems and smart cities; and the CeNSE project by HP Labs, illustrated on the exploitation of a worldwide sensor network in order to create a "central nervous system for the Earth". By the equivalent time the technologies that will allow the integration are being developed and tested. For example, the LowPAN standard, defined by IETF [2], allows the transmission of IPv6 packets during computationally confidential networks. Moreover, it is actually possible to link the data produced by the elements of a WSN (sensor nodes) with web services based on SOAP and REST, messaging mechanisms (such as emails and SMS) or social networks (e.g. Twitter) and blogs (e.g. Wordpress) [3]. However, having IP connectivity does not mean that every sensor node should be directly connected to the Internet. Here, many challenges that must be carefully considered, and one of those disputes is security. While in this paper we will introduce some of the most important security integration challenges (integration of security mechanisms and services, data privacy) we will focus on one specific challenge: the concrete connectivity model between the WSN and the Internet.

II.SECURITY INTEGRATION CHALLENGES

In order to allocate wireless sensor network turn into an essential part of the IoT in a secure way, several security challenges must be considered. As aforementioned, in this paper we focus on the connectivity at the network level. Nevertheless, there are additional security challenges that, even if they are not studied in this paper, must be highlighted to guide future work. These challenges are tightly related to WSN, but also can be applicable to other relevant technologies of the IoT. Some of the most important challenges are the integration of security mechanisms and users" acceptance. It is essential to consider the security of the IoT from a global perspective and not as a set of isolated issues related to specific technologies. Otherwise, we could reach a point where a technology (e.g. a WSN) satisfies a minimal set of security requirements, but its integration with other technologies (e.g. RFID) generates new requirements

which had not been previously considered. Regarding the users perspective, the IoT must be able to satisfy their expectations without betraying their trust. Not only the IoT must be useful, but also users must perceive that they control any information that is related to them. If users feel that they are controlled by the system, or they have a false perception of security which is betrayed due to a violation of their rights, any advantage that the IoT can provide will be directly rejected. Data privacy must also be critically considered. The information obtainable concerning a exacting user will not only consist of his personal data, but also of any data generated by the objects (e.g. sensor nodes) surrounding the individual. In this situation, it is necessary to clarify who owns the data and how the user can be sure that the data is safe and will not be used without his consent. Moreover, there will be some scenarios where part of the data should be shared in order to provide a service. For example, in case of disaster, a person should present her health data (e.g. personal history and allergies) to the ambulance and medical staff in a transparent way. Beyond individual users, data privacy is also a matter of concern for business scenarios. Any company that makes use of the mechanisms provided by the IoT will generate a huge data flow (e.g. human resources interaction, production processes). Such data must remain private, illicit by the company and accessible only when required. Finally, another significant aspect that must be taken into account is the protection of the components of the IoT by means of adequate security mechanisms. This not only refers to the use of security protocols and mechanisms at the network level (which will be considered in the remainder of the paper), but also to the interactions between objects and services. As the IoT is a distributed, dynamic and heterogeneous infrastructure, it is essential to separate a number of technologies, protocols and access models in order to provide services in an appropriate way. From a security viewpoint, the primary objects and infrastructures must be able to handle several identification and security mechanisms in a transparent and scalable way. Although there will exist some isolated scenarios (e.g. a digital home, the headquarters of a company) where interactions between objects will be kept under-control, It will exist different services (such as logistics) which will make use of several elements geographically dispersed all over the world. Due to this, reaching an equilibrium point in the secure interactions between objects and services is one of the most interesting challenges in the IoT [6].

III.COMMON ISSUES IN INTERNET OF THINGS (IOT)

- *Scalability:* - The IoT has larger overall scope than communications with conventional hosts. There will be small (home environment) or large scale (factory, building) application area. Objects communicate with each other and with people seamlessly. Each constituent might be offering different services. Basic functionalities such as communication, service discovery need to be functioning efficiently in both small and large scale environment. Scalability regarding addressing can be taken as an example. IPv4 address is finishing, object-to-object communication needs huge number of IP addresses in order to uniquely identify each objects. As a scalable solution, IPv6 can be used which can accommodate as many things as required to include in the IoT.

- *Interoperability:* - World of physical objects is extremely diverse. They have different communication, information and processing capabilities. Each object would also be subjected to very different conditions such as power energy vailability and communication bandwidth requirement. In order to facilitate communication and cooperation common practices and standards are required. Interoperability issue includes device, services heterogeneities. Devices are small, large, with continuously powered, without power supply. Interoperability solution should be maintained to provide seamless interaction among them. Service description, publishing, and discovery mechanisms should be interoperable otherwise the IoT will be converted into islands of heterogeneous object network.
- *Discovery:* - In dynamic environment of ubiquitous networking, suitable services for objects must be automatically identified. As users want to know product information and their availability all the time, it requires appropriate semantic means of describing their functionality.
- *Data Volumes:* - Depending on application and use cases there is variance in data volume. In a

scenario where there is brief collaboration among objects data volume will be less. However, in case where there are large number of objects and interact among very frequently there are large volume of data.

How to handle big volume of data is one of the important challenges of ubiquitous networking.

Volume can be considered either from device or as a whole network perspective. Each object has augmented memory, storage and processing capability. If there are a large number of peer objects communicating with each other, object runs out of processing, memory and storage. From network perspective it is also difficult to handle bulk amount of data if objects produce huge bytes of data regularly. Solution can be periodic communication between objects or some data compression and optimization techniques.

- *Power Supply:* - Scope of object is broad in the IoT. It ranges from small to large. Moreover, things move around and difficult to connect to power supply all the time. So they need to operate with self-sufficient energy source. Passive RFID does not contain power supply, which requires reader in order to get information from it. Not all objects can be connected to continuous power supply also, providing battery for each small object may not be feasible. Therefore, energy efficient communication mechanisms are essential.
- *Fault-Tolerance:* - The IoT consists of objects have less power. They are more dynamic and mobile compare to current state. However, users rely and believe that network will function properly. To maintain robust and trust worthy dynamic ubiquitous networking requires redundancy in several levels and ability to automatically adapt to changed conditions depending on the required quality of service.
- *Security and personal privacy:* - Users are fighting with security and privacy issue of current in large extent. When it will be broaden in to ubiquitous networking, there is even more threat of security and personal privacy. Confidentiality, authenticity and trustworthiness communication partners need to be maintained. Users may want to give things limited service access not allowing them to communicate in uncontrolled manner.
- *Device adaptation:* - Initially started with retail and logistic application, the IoT is covering very general applications scenario integrating things to the network. It allows objects to collaborate each other and with person. There are heterogeneous devices, application scenarios, data format, and communication network. Each connected objects should be able to adapt the situation where it is now. When a person with smart phone enters home, it should adapt communication mechanism, addressing and localized environment. When it reaches in office environment it should adapt with new situation where the mechanisms available in home can be different. Adaption in many senses should be maintained.

IV. EXISTING SYSTEM

Zhang et al. [4] presented a suite of novel schemes that can ensure data confidentiality against master nodes and also enable the network owner to verify with very high probability the authenticity and completeness of any query result by inspecting the spatial and temporal relationships among the returned data. Detailed performance evaluations confirm the high efficacy and efficiency of the proposed schemes.

Cordasco and Wetzel [5] demonstrated the results of implementation and evaluation of both protocols on real resource-limited hardware. The expected difference

between
the two protocols was shown to be consistent with this real
world scenario. These experiments showed that there is
significant room between the two protocols for a secure hybrid protocol to be developed which takes advantage of the
strongest points of both. Future work needs to delve further into the extensive body of work on various trust metrics. This includes the testing of other trust metrics for use in ad-hoc routing as well as developing the aforementioned hybrid protocols and testing their performance against the results presented in this paper. In addition, it is necessary to test the quality of the routing decisions produced by all of these protocols in a malicious environment.

Internet Yu et al. [6] analyzed a novel yet important issue of fine-
grained data access control for distributed storage in WSNs. To address the problem, they proposed a scheme called FDAC in which each sensor node is assigned a set of attributes, and each user is assigned an access structure which designates the access capability of the user. The sensor data is encrypted under the attributes such that only the users with the intended access structure are able to decrypt.

Ning et al. [7] developed message specific puzzles, a weak
authentication mechanism, to mitigate DoS attacks against
signature-based and µTESLA-based broadcast authentication
in wireless sensor networks. This approach has a number of
nice properties: First, a weak authenticator can be efficiently
verified by a regular sensor node, but takes a computationally
powerful attacker a substantial amount of time to forge.
Second, a weak authenticator cannot be pre-computed without
a non-reusable (or short-lived) key disclosed only in a valid
broadcast packet. Thus, an attacker cannot start the expensive
computation to forge a weak authenticator without seeing a
valid broadcast packet. Third, even if an attacker has sufficient
computational resources to forge one or more weak
authenticators, it is difficult to reuse these forged weak
authenticators. Thus, this weak authentication mechanism
substantially increases the difficulty of launching successful
DoS attacks against signature based and µTESLA-based
broadcast authentication.

Zhang et al. [8] developed a formal framework and theory
to investigate the correctness, optimality, inter-operatively of
trust-based routing protocols for WANETs. Their results
obtained here can be extended in two ways. (1) For indirect
trust inference problems, they only consider the situation when
all trusts in a WANET are transitive. When transitive and no
transitive trust coexist in a WANET, a new

and any cast are totally different from that for unicast, and the
concept of path selection will be replaced by tree selection. Therefore, these topics should be further investigated.

Marti et al. [9] have used a watchdog that identifies
misbehaving nodes and a patl~rater that helps routing protocols avoids these nodes. Through simulation they evaluate watchdog and pathrater using packet throughput, percentage of overhead (routing) transmissions, and the
accuracy of misbehaving node detection. When used together
in a network with moderate mobility, the two techniques
increase throughput by 17% in the presence of 40%
misbehaving nodes, while increasing the percentage of
overhead transmissions from the standard routing protocol's
9% to 17%. During extreme mobility, watchdog and pathrater
can increase network throughput by 27%, while increasing the
overhead transmissions from the standard routing protocol's
12% to 24%.

Zakhary et al. [10] discussed how they integrate two kinds of centrality in their reputation-based protocol and propose a number of optimizations for more efficient node monitoring and trust resolution such as selective deviation test and adaptive expiration timer. Their early prototype
implementation over AODV confirms and extends the results published. The results presented in this paper show that the throughput remains above 70% in the presence of the
increasing number of black hole nodes while the jitter

algebraic structure for a combined trust metric is needed and consequently new algorithm should be designed to infer indirect trust under no transitive trust constraints. (2) From routing‟ s point of view, in their framework they only consider topology-based routing protocols. They can extend their study to location-based routing like geographic routing, which is popular for WANETs. Also in this paper they restrict ourselves to unicast routing. Obviously, the trust metrics for multicast, broadcast,

and delay decrease and are below AODV. They also discuss the impact the distribution of centrality and reputation of their nodes has on the time needed to isolate malicious nodes. Their subsequent work will focus on studying the impact of centrality and configuration parameters on the protocol performance in relation to network throughput, network delay, network jitter and the protocol detection ratio.

Szabo and Hauert [11] considered: the risk adverse loners who are unwilling to participate in the social enterprise and rather rely on small but fixed earnings. This results in a rock-scissors-paper type of cyclic dominance of the three strategies. In the prisoner‟ s dilemma, the effects of voluntary participation crucially depend on the underlying population structure. While leading to homogeneous states of all loners in well-mixed populations, they demonstrate that cyclic dominance produces self-organizing patterns on square lattices but leads to different types of oscillatory behavior on random regular graphs: the temptation to defect determines whether damped, periodic, or increasing oscillations occur. These Monte Carlo simulations are complemented by predictions from pair approximation reproducing the results for random regular graphs particularly well.

Szabo et al. [12] have exhibited a phase transition from a mixed state of cooperators and defectors to a homogeneous one where only the defectors remain alive. Using systematic Monte Carlo simulations and different levels of the generalized mean-field approximations they have determined the phase boundaries (critical points) separating the two phases on the plane of the temperature (noise) and temptation to choose defection. In the zero temperature limit this analysis suggests that the cooperation can be sustained only for those connectivity structures where three-site clique percolation occurs.

V. FEATURES OF THE IOT

- *Overall aspects:-* (Order(s) of magnitude bigger than the Internet, No computers or humans at endpoint, Inherently mobile, disconnected, unattended)
- *Applications/services aspects:-* There are many use cases among various stakeholders in IoT environment. Each device/machine can be used for multiple applications/services with different characteristics.
- *Networking aspects:-* It is required to provide a common communications technology that supports all applications/services as well as heterogeneous
- *Link/physical layer aspects*:- There are various types of networking interfaces which have different coverage and data rates. These environments have the characteristics of low power and lossy networks like Bluetooth, IEEE 802. 15.4 (6LoWPAN, ZigBee), NFC etc.
- *Smart/connected bjects aspects:-* Smart/connected objects are heterogeneous with different sizes, mobility, power, connectivity and protocols. A physical object interacts with several entities, performs various functionalities and gener ates data that might be used by other entities. Usually resources of these objects are limited.
- *Smart environment aspects:-* Smart environment which consists of networks of federated sensors

and actuators can be extended from homes/offices to buildings/cities.From residential home, end-to-end large scale services such as smart cities can be considered.

VI. CONCLUSION

It is apparent that the potential of the wireless sensor networks (WSN) paradigm will be completely unleashed once it is connected to the Internet, fetching part of the Internet of Things (IoT). The Internet of Things (IoT) presented the insurrection already below way that is seeing a growing number of internet enabled devices which can network and converse with each other and with other web-enabled gadgets.
IoT refers to a state where Things (e.g. objects, environments, vehicles and clothing) will have more and more information connected with them and may have the aptitude to sense, communicate, network and produce new information, flattering an integral part of the Internet."

REFERENCES

[1]IBM: A Smarter Planet, http://www.ibm.com/smarterplanet/, Accessed on October 2010.
[2]G. Montenegro, N. Kushalnagar, J. Hui, D. Culler. RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks. 2007
[3]Libelium: Interfacing the Sensor Networks with the Web 2.0, http://www.libelium.com/, Accessed on October 2010
[4] R. Zhang, J. Shi, Y. Zhang, and J. Sun, "Secure cooperative data storage and query processing in unattended tiered sensor networks," IEEE J. Sel. Areas Commun., Vol. 30, No. 2, pp. 433-441, 2012
[5] J. Cordasco and S. Wetzel, "Cryptographic versus trust-based methods for MANET routing security," Electron. Notes Theor. Comput. Sci., Vol. 197, No. 2, pp. 31-140, 2008
[6] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," in Proc. IEEE INFOCOM, pp. 963-971, 2009
[7] P. Ning, A. Liu, and W. Du, "Mitigating DoS attacks against broadcast authentication in wireless sensor networks,"ACMTrans. Sensor Netw., Vol. 4, No. 1, pp.1-35, 2008
[8] C. Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study of trust-based routing in wireless ad hoc networks," in Proc. IEEE INFOCOM, pp. 1-9, 2010
[9] S. Marti, T. Giuli, K. Lai, M. Baker et al., "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Ann. Int. Conf. Mobile Comput. Netw., ACM, pp. 255-265, 2000
[10] S. Zakhary and M. Radenkovic, "Reputation-based security protocol for manets in highly mobile disconnection-prone environments," in Proc. 7th Int. Conf. Wireless On-demand Netw. Syst. Serv., 2010
[11] G. Szabó and C. Töke, "Evolutionary prisoner" s dilemma game on a square lattice," Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top., vol. 58, no. 1, pp. 69-74, 1998.
[12] G. Szabó, J. Vukov, and A. Szolnoki, "Phase diagrams for an evolutionary prisoner" s dilemma game on two-dimensional lattices," IEEE Trans. Mobile Comput., vol. 72, no. 4, p. 047107, 2005.