A security model for Wireless Sensor Networks

A. Aliti[1], and K. Sevrani[2]
[1] South East European University, Tetovo, Macedonia
[2]University of Tirana, Tirana, Albania
aa03511@seeu.edu.mk, kozeta.sevrani@unitir.edu.al

***Abstract* – State-of-the-art security frameworks have been extensively addressing security issues for web resources, agents and services in the Semantic Web. The provision of Stream Reasoning as a new area spanning Semantic Web and Data Stream Management Systems has eventually opened up new challenges. Namely, their decentralized nature, the metadata descriptions, the number of users, agents, and services, makes securing Stream Reasoning systems difficult to handle. Thus, there is an inherent need of developing new security models which will handle security and automate security mechanism to a more autonomous system that supports complex and dynamic relationships between data, clients and service providers. We plan to validate our proposed security model on a typical application of stream data, on Wireless Sensor Networks (WSNs). In particular, WSNs for water quality monitoring will serve as a case study. The proposed model can be a guide when deploying and maintaining WSNs in different contexts. Moreover, this model will point out main segments which are most important in ensuring security in semantic stream reasoning systems, and their inter-relationships. In this paper we propose a security framework to handle most important issues of security within WSN. The security model in itself should be an incentive for other researchers in creating other models to improve information security within semantic stream reasoning systems.**

Keywords – wsn security; security framework; security model; authentication, inference

I. INTRODUCTION

The Web is highly dynamic: new information is constantly added, and existing information is continuously changed or removed. It has been estimated that every minute on the Internet 600 videos are uploaded on YouTube, 168 million e-mails are sent, 510,000 comments are posted on Facebook and 98,000 tweets are delivered in Twitter [23]. In these scenarios information changes at a very high rate, so that we can identify a stream of data on which we are called to operate with high efficiency. In the last few years, several researchers and practitioners have proposed solutions for processing streams of information on-the-fly, according to some pre-deployed processing rules or queries [14]. This led to the development of various Data Stream Management Systems (DSMSs) [15] and Complex Event Processing (CEP) systems [17] [16] that effectively deal with the transient nature of data streams, providing low delay processing even in the presence of large volumes of input data generated at a high rate. However, DSMSs lack the support of performing complex reasoning tasks, CEP do not support reasoning, while Semantic Web caches all the knowledge base. As a result, a number of recent works propose to unify reasoning and stream processing, giving birth to the research field of Stream Reasoning [6]. In 2009, stream reasoning was defined as an "unexplored yet high impact research area". A number of its implementations are currently in place including C-SPARQL [21], StreamRule [20], StreamJess [8], C-SWRL [9], ETALIS [18], EP-SPARQL [19] etc.

Typical applications of stream data are Wireless Sensor Networks (WSNs). WSNs are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as water quality, temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. Modern approaches are bi-directional, also enabling control of sensor activity [10].

There is a need to develop a model which would provide Semantic Web services that are relevant to the user request, and only to those users who have got the access rights. Different authors have indicated different aspects that should be considered while designing an access control mechanism for the Semantic Web services [11]. For instance, [11] points out the need that Access Control Mechanism should satisfy composite web services. The author afterwards turns the focus on semantic relations among concepts, than the incorporation of policies in Access Control. He also emphasizes the need to consider credentials, and at the end the fact that authorization should be considered over authentication, etc. Thus, there is an inherent need for a unique mechanism or model that is able to satisfy the complex requirements of an access control of WSN network.

When creating a WSN network, many times we see a focus on data encryption, which is important too. But, say after successful encryption of data chances of device itself being hacked still exist. If there is no way to establish the authenticity of the data being communicated to and from certain WSN node, security is compromised [22]. For example, if we build a temperature sensor for smart homes. Even though you encrypt the data it transfers, if there is no way to authenticate the source of data then anyone can make up fake data and send it to your sensor instructing it to cool the room even when its freezing or vice versa. Authentication issues may not be upfront but they definitely pose a security risk. There are several

researches in this direction, more notably in recent years the PAuthKey authentication scheme. They propose a pervasive lightweight authentication and keying mechanism for WSNs in distributed Internet of Things (IoT) applications, in which the sensor nodes can establish secured links with peer sensor nodes and end-users. The established authentication scheme PAuthKey is based on implicit certificates and it provides application level end-to-end security.

In WSNs we also need secure XML. According to [12], access must be controlled to various portions of the document for reading, browsing and modifications. There is research on securing XML and XML schemas. The next step is securing RDF (Resource Description Framework). Now with RDF not only do we need secure XML, we also need security for the interpretations and semantics.

We also need to examine the inference problem for the Semantic Web. Inference is the process of posing queries and deducing new information. It becomes a problem when the deduced information is something the user is unauthorized to know. With the Semantic Web, and especially with data mining tools, one can make all kinds of inferences [13].

There are hardware issues also. From the very beginning the internet of things hardware has been the problem. The problem is with modern architecture of the chips made specifically for the IoT devices, the prices will go up making them expensive. Also the complex design will require more battery power which is definitely a challenge for IoT applications. Affordable wearable IoT devices will not use such chips meaning there is need for better approach [22].

While there are dozens of research in different aspects of security within Semantic Web applications in general and WSNs in particular, like the ones described by [4], [1], [2], [3] and [5], there is still no integrative model which takes in consideration different segments of security within WSNs. In this research we aim to create a unique security model, which could be implemented anytime we need to deploy new WSN system. The idea is to firstly validate the model on WSNs for water quality monitoring and then in other domains. Finally, we will generalize the findings of the research, and make the model applicable in different stream reasoning domains.

II. AIMS OF THE MODEL

The main aim of this research work is to develop an integrative security model for stream reasoning systems in general and WSNs in particular. In our model, we try to include at least these segments: secrecy, privacy, authentication, authorization, encryption and inference.

The research sub goals include security issues on data, semantic security and secure information integration, which are components of the secure Semantic Web and thus stream reasoning within WSN.

III. HYPOTHESES

We have come up with two hypotheses which concern the quantitative part of the research, and two research questions for the qualitative part of the research.

Hypotheses:

- Creation of an integrative security model for stream reasoning systems in general and WSNs in particular will improve security in steam reasoning systems.
- Current approaches to security within WSNs are isolated and not completely efficient for WSNs.

Research Question 1: Are current security foundations of Semantic Web also relevant for Stream Reasoning systems?

Research Question 2: Are current Semantic Web security measures valid for the data, ontologies and rules layer of the stream data applications?

IV. RESEARCH METHODOLOGY

This research employs mixed method approach. We use qualitative methods when analyzing different findings on security within WSN, and we use quantitative methods when we conduct observation and experimentation in the acquisition of new knowledge.

The model of the research will be organized with the following hierarchy of tasks:

- *Task 1. Security models on Semantics Web Applications*. A research on Semantic Web Security Issues and privacy mechanisms will be done at this task.
- *Task 2. Security aspects on WSNs.* A research on main security aspects of WSNs will be done at this task.
- *Task 3. Analysis of WSNs and DSMS security models.* The works on this task will identify the appropriate security issues and mechanisms applicable on the domain of Stream Reasoning within WSNs.
- *Task 4. Build a valid and consistent security model for WSNs.* This is the main thesis task. We will build a valid and consistent security model based on the best practices on Semantic Web and DSMSs, and outline specific security and privacy mechanisms for the domain of WSNs.
- *Task 5. Validate the model on Stream Reasoning systems.* The model build on Task 4 will be validated in others stream reasoning domain.

V. TENTATIVE MODEL AND CONTRIBTION

Based on the research so far and literature review, our model will have these components: Authentication, Authorization, Encryption, Privacy, Inference Security, Physical security.

While all these components have their own importance, the idea is to test the model in the real world, and prioritize components by comparing in which scenarios - which components are more vulnerable and need more attention. As the research progresses, the number of components of the model might increase or decrease, and the priority of the components can be re-organized. At “Fig.1” there are presented the components of the model.

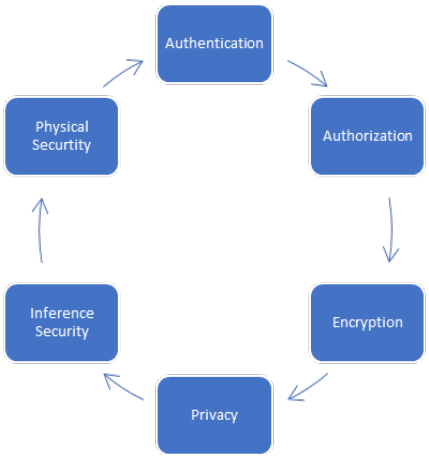

Figure 1. Components of the model

In the research to follow, we plant to do thorough analysis for each component, and their inter-relationships, and how that affects the overall security of a WSN network.

The design of an integrative security model for WSNs and stream reasoning systems will contribute on the community of Semantic Web and stream reasoning. Namely, our model can be a guide when deploying and maintaining WSNs in different contexts. The model will be validated on WSNs for water quality monitoring and other similar sensor networks. We have chosen water quality because of previous research that has been completed on it, on which data we plan to do additional analysis [8].

We think it is very important to create an integrative security model for stream reasoning systems in general, and WSNs in particular, because that will improve security in stream reasoning systems. Secondary, this model will point out main segments which are most important in ensuring security in semantic stream reasoning systems, and their inter-relationships.

Another contribution will be thorough analysis of current approaches to security. We intend to confirm that focusing on certain segment and overlooking other segments of security contributes to semantic stream reasoning systems being vulnerable to security breaches. These analyses in turn should be an important part of the contribution.

As we intend to research if current security foundations of Semantic Web are also relevant for Stream Reasoning systems, we hope to come up with valuable findings in this direction too.

Both qualitative part and quantitative parts of the research should result with important findings, which should also contribute in future directions of research in security in semantic stream reasoning systems. The security model in itself should be an incentive for other researchers in creating other models to improve information security within semantic stream reasoning systems.

VI. CONCLUSIONS

This research will strive to create an integrative security model for stream reasoning systems and WSNs. In our model, we will try to include at least these segments: Authentication, Authorization, Encryption, Privacy, Inference Security, Physical security.

The WSNs continue to grow and become widely used in many mission-critical applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, as well as unreliable communication and unattended operation, etc [4].

Traditional security models do not provide adequate protection in this dynamic and open environment that is WSNs. While there are significant efforts under way that should make WSNSs more secure, there is a lack of a model which takes into consideration all main aspects of security.

We hope to develop and implement a security model which has all main segments of security for stream reasoning systems, and which can be used when we deploy or need to maintain a WSN in different contexts. While creating this network we aim to evaluate authentication, access control, inferences, etc, and try to mitigate against any threats related to these components.

REFERENCES

[1] B. Thuraisingham, “Security Issues for the Semantic Web”, in Proceedings of the 27th Annual International Computer Software and Applications Conference. IEEE 2003, p. 632.

[2] L. Kagal, T. Finin and A. Joshi, “A Policy Based Approach to Security for the Semantic Web” in 2nd International Semantic Web Conference (ISWC2003), September 2003.

[3] F. Scilla and M. N. Huhns. “Making Agents Secure on the Semantic Web ” In IEEE Internet Computing (2002): pp. 76-93.

[4] K. Chelli, “Security Issues in Wireless Sensor Networks: Attacks and Countermeasures” in Proceedings of the World Congress on Engineering 2015 Vol I WCE 2015, July 1 - 3, 2015, London, U.K.

[5] A. Medic and A. Golubovic, “Making secure Semantic Web” in Universal Journal of Computer Science and Engineering Technology, Vol. 1 No. 2, 2010, pp. 99-104.

[6] A. Margara, J. Urbani, F. v. Harmelen, H. Bal, “Streaming the web: Reasoning over dynamic data” in Web Semantics: Science, Services and Agents on the World Wide Web, 25(0): 2014, pp. 24 – 44.

[7] E. D. Valle, D. Dell’Aglio and A. Margara, “Tutorial: Taming Velocity and Variety Simultaneously in Big Data with Stream Reasoning” in: The 10th ACM International Conference on Distributed and Event-Based Systems, Irvine, USA, June 20-24, 2016.

[8] E. Jajaga, L. Ahmedi and F. Ahmedim, “StreamJess: Stream Data Reasoning System for Water Quality Monitoring” in Intl. J. of Metadata, Semantics and Ontologies, IJMSO, 11(4), 2016, pp. 207–220.

[9] E. Jajaga, and L. Ahmedi, “C-SWRL: SWRL for Reasoning over Stream Data”, in First International Workshop on Semantic Data Integration (SDI '17) in conjunction with The Eleventh IEEE International Conference on Semantic Computing. San Diego, California, USA. Jan 30 - Feb 1, 2017.

[10] M. Zanjireh, H. Larijani, “A Survey on Centralised and Distributed Clustering Routing Algorithms for WSNs ” in IEEE 81st Vehicular Technology Conference. Glasgow, Scotland: IEEE. Spring 2015.

[11] M. Gondara "Access Control Mechanisms for Semantic Web services - a discussion on requirements and future directions", 2011.

[12] N. Hamid, "Techniques and Applications for Advanced Information Privacy and Security", 2009.

[13] S. Vimercati, R. Indrakshi, I. Ray, "Data and Applications Security XVII: Status and Prospects", 2009

[14] G. Cugola, A. Margara, "Processing flows of information: From data stream to complex event processing", ACM Comput. Surv. 44 (3), 2012.

[15] B. Babcock, S. Babu, M. Datar, R. Motwani, J. Widom, "Models and issues in data stream systems" ub Proceedings of the twenty first ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems. PODS '02. ACM, New York, NY, USA, 2002, pp. 1–16.

[16] O. Etzion, P. Niblett "Event Processing in Action, 1st Edition. Manning Publications Co., Greenwich, CT, USA. (2010)

[17] Luckham, D. C., The Power of Events: An Introduction to Complex Event Processing in Distributed Enterprise Systems. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA. (2001)

[18] D. Anicic, D., P. Fodor., R. Rudolph, R. Stuhmer, N. Stojanovic, R. Studer, "A Rule-Based Language for Complex Event Processing Reasoning" in Proceedings of the Fourth International Conference on Web reasoning and rule systems, Springer-Verlag Berlin, Heidelberg, 2010, pp. 42-57.

[19] D. Anicic, P. Fodor, S. Rudolph, N. Stojanovic "EP-SPARQL: A Unified Language for Event Processing and Stream Reasoning", in: WWW 2011, 2011, pp. 635-644.

[20] A. Mileo, A. Abdelrahman, S. Policarpio, M/ Hauswirth, "StreamRule: A nonmonotonic stream reasoning system for the semantic web", in: Faber, W., Lembo, D. (eds.) RR 2013. LNCS, vol. 7994, Springer, Heidelberg, 2013, pp. 247–252.

[21] D. F. Barbieri, D. Braga, S. Ceri, E. D. Valle and M. Grossniklaus, 'C-SPARQL: a continuous query language for RDF data streams', in International Journal of Semantic Computing, Vol. 04 No. 01, 2010, pp. 3–25.

[22] S. Singh "IoT Security-Issues, Challenges and Solutions", 2016

[23] Go-Gulf 2017, "60 Seconds – Things That Happen On Internet Every Sixty Seconds [Infographic]" viewed 26 July 2017, <https://www.go-gulf.com/blog/60-seconds/>

[24] T. G. Stavropolus "Integrating sensors, multimedia and semantinc analysis for the ambient care of dementia. Pervasive and Mobile Computing", 2016, pp. 1-2.

[25] O.M Latava "Security risk visualization with semantic risk model", in Second International Workshop on Mobile Cloud Computing systems, Menagement and Security, 2016, pp. 3-5.

[26] S. Zhu, "Establishing Pairwise Keys for Secure Communication in Ad Hoc Networks: A probabilistic Approach", in 11th IEEE International Conference on Network Protocols, 2016 pp. 2-3.

[27] J. Kong, "Providing Robust and Obiquitous Security Support for Mobile Ad-Hoc Networks" in IEEE, 2001, pp. 3-4.

[28] K. Sazgiri, "A Secure Routing Protocol for Ad Hoc Netwoks", 10th IEEE International Conference, on Network Protocols, 2001, pp. 2-3.

[29] D. Ghosh, "Privacy control in smart phones using semantically rich reasoning and context modeling", IEEE, 2013, pp. 2-3.

[30] M. Guiziani, "Security and Trust in Mobile Ad Hoc Networks," in 4th Annual Communication Networks and Services Research Conference, 2006, pp. 3-4.

[31] Sh. W.Shieh, "Ad Hoc and P2P Security " in IEEE Computer Society, 2016, pp. 14-15.

[32] G. D. Modica, "Matchmaking semantic security policies in heterogeneous clouds" in Future Generation Computer Systems, Volume 55, 2016, pp. 176-185.

[33] F. Shang, "Distributed controllers multi-granularity security communication mechanism for software-defined networking", in Computers & Electrical Engineering, In press, corrected proof, 2017, pp. 35-38.

[34] Z. Babovic "Novel System Architectures for Semantic-Based Integration of Sensor Networks, Advances in Computers, Volume 90, 2013, pp. 91-183.

[35] H. UgurYildiz, "Maximizing Wireless Sensor Network lifetime by communication/computation energy optimization of non-repudiation security service: Node level versus network level strategies" in Elsevier B.V, Volume 37, Part 2, 2016, pp. 301-323.

[36] R. L. Gilaberte, "A secure routing protocol for ad hoc networks based on trust" in IEEE Computer Society, 2007, pp. 9.

[37] F. Bamashmoos, "Towards Secure SPARQL Queries in Semantic Web Applications Using PHP" in IEEE Computer Society, pp. 276-277.

[38] D. Jeong "SS-RBAC: Secure Query Processing Model for Semantic Sensor Networks, Future Generation Communication and Networking" 2008. FGCN '08. Second International Conference, pp. 352-355.

[39] D. Macedonio, "A semantic analysis of key management protocols for wireless sensor networks, Cryptography and Security", 2011, 202-203.

[40] R. H. Jhaveri , "DoS Attacks in Mobile Ad Hoc Networks: A Survey" in Advanced Computing & Communication Technologies (ACCT)", 2012.

[41] A. Wasef , "EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks " in IEEE Transactions on Mobile Computing, Volume: 12, Issue: 1, 2011, pp. 78-89.

[42] H. Xia, "Trust prediction and trust-based source routing in mobile ad hoc networks", in Elsevier B.V., Volume 11, Issue 7:, 2013, pp. 2096-2114.

[43] E. Y. Vasserman, "Vampire attacks: Draining life from Wireless and Ad Hoc Sensor Networks" IEEE Transactions on Mobile Computing (Volume: 12, Issue: 2, 2013, pp. 318-332.

[44] A. Razzaq, "Semantic security against web application attacks" in Information Sciences, Volume 254, 2013 pp. 19-38.

[45] G. Modica, "Matchmaking semantic security policies in heterogeneous clouds" Future Generation Computer Systems, Volume 55, 2016, pp. 176-185.

[46] S. S. Alqahtani, "Tracing known security vulnerabilities in software repositories – A Semantic Web enabled modeling approach" in Science of Computer Programming, Volume 121, 2016, pp. 153-175.

[47] G. Denkera "Security in the Semantic Web using OWL, Information Security Techical Report", Volume 10, Issue 1, 2003, pp. 51-58.

[48] H. Hendre, "A semantic Approach to Cloud Security and Compliance" IEEE Cloud Conference, New York, 2015, pp. 34-37.

[49] B. Mokhtar, "Survey on Security Issues in Vehicular Ad Hoc Networks" in Alexandria Engineering Journal, 2015, pp. 1116-1119.