Oct 27th, 1:20 PM - 2:30 PM

A need for an integrative security model for semantic stream reasoning systems

Admirim Aliti
EduSoft

Edmond Jajaga
EduSoft, edmond@edusoft.com.mk

Kozeta Sevrani
EduSoft

A need for an integrative security model for semantic stream reasoning systems

Admirim Aliti[1], Edmond Jajaga[2], Kozeta Sevrani[3]

[1]South East European University aa03511@seeu.edu.mk
[2]EduSoft, StivNaumov 1/1-1, Skopje, Republic of Macedonia
edmond.jajaga@ubt-uni.net
[3]University of Tirana, 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, make 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. In this paper, we describe initial findings regarding state-of-the-art approaches and how they investigate different aspects of security within Wireless Sensor Networks, which is a typical example of Stream Reasoning systems.

Keywords: WSN, Security, stream data, encryption, reasoning.

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 [1]. 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 [2]. This led to the development of various Data Stream Management Systems (DSMSs) [3] and Complex Event Processing (CEP) systems [4] 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 [5]. 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 [7], StreamRule [8], StreamJess [9], C-SWRL [10], ETALIS, EP-SPARQL, etc.

Literature Review: Initial findings

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 [11].

The Semantic Web in general, and WSNs in particular, create new security challenges due to their completely decentralized nature, the meta data descriptions, the number of users, agents, and services. Security challenges associated with the Semantic Web involves the ability to handle security and to automate security mechanism to a more autonomous system that supports complex and dynamic relationships between data, clients and service providers.

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 [12]. For instance, Gondara[12] points out the need that Access Control Mechanism should satisfy composite web services, than turns the focus on semantic relations among concepts, than the incorporation of policies in Access Control, than credentials consideration, than 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.

Security can be violated if access control to each node in the WSN network is considered separately ignoring the interrelationships among nodes [12]. Information may be inaccessible to authorized subjects if links among nodes are not considered. An access control to the WSN network needs to additionally ensure that all the information authorized for view should be revealed to a subject.

Current approaches - isolated

We view access control policies as conditions that a node defines to restrict the number of users who may access the functionalities offered by the device. Establishing the requirements of an access control mechanism for Semantic Web services is a critical milestone in the development of a security model for Stream Reasoning systems in general, and WSNs in particular. Our vision is to create a security model which will be proposed for different WSNs. WSNs employed for water quality monitoring will serve as a case study for the research.

Research Methodology

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 Thuraisingham [13], Kagal et al. [14], Scillaand Huhns [15] and Medic and Golubovic [16], there is still no integrative model which takes in consideration different segments of security within WSNs. As we aim to create a unique security model, the solution could be implemented anytime needing

to deploy new WSN system. We need to analyze security aspects on WSNs and also analysis of Semantic Web. Validate the model on our Stream Reasoning systems (C-SWRL and StreamJess). 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.

Conclusion

The WSNs continue to grow and become widely used in many mission-critical applications. So, the need for security becomes vital. However, the WSNs suffer from many constraints such as limited energy, processing capability, and storage capacity, as well as unreliable communication and unattended operation, etc [17]. 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 strive 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 such threats.

References

1. 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/>
2.
3. Cugola, G., Margara, A., Jun, Processing flows of information: From data stream to complex event processing. ACM Comput. Surv. 44 (3), 15:1–15:62. (2012)
4. Babcock, B., Babu, S., Datar, M., Motwani, R., Widom, J., Models and issues in data stream systems. In: Proceedings of the twenty first ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems. PODS ’02. ACM, New York, NY, USA, pp. 1–16. (2002)
5. 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)
6. Margara, A., Urbani, J., van Harmelen, F., Bal, H., Streaming the web: Reasoning over dynamic data. Web Semantics: Science, Services and Agents on the World Wide Web, 25(0): 24 – 44 (2014)
7. Della Valle, E., Dell’Aglio, D., and Margara, A., 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. Barbieri, D. F., Braga, D., Ceri, S., Della Valle, E. and Grossniklaus, M.: ‘C-SPARQL: a continuous query language for RDF data streams’, International Journal of Semantic Computing, Vol. 04 No. 01, pp. 3–25 (2010)

9. Mileo, A., Abdelrahman, A., Policarpio, S., Hauswirth, M.: StreamRule: A nonmonotonic stream reasoning system for the semantic web. In: Faber, W., Lembo, D. (eds.) RR 2013. LNCS, vol. 7994, pp. 247–252. Springer, Heidelberg (2013)
10. Jajaga, E., Ahmedi, L., and Ahmedi, F., StreamJess: Stream Data Reasoning System for Water Quality Monitoring. Intl. J. of Metadata, Semantics and Ontologies, IJMSO, 11(4), pp. 207–220. (2016)
11. Jajaga, E. and Ahmedi, L.: C-SWRL: SWRL for Reasoning over Stream Data. 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.
12. Zanjireh, M., Larijani, H., A Survey on Centralised and Distributed Clustering Routing Algorithms for WSNs (PDF). IEEE 81st Vehicular Technology Conference. Glasgow, Scotland: IEEE. Spring 2015.
13. Gondara, M., Access Control Mechanisms for Semantic Web services - a discussion on requirements and future directions (2011)
14. Thuraisingham, B., Security Issues for the Semantic Web. In Proceedings of the 27th Annual International Computer Software and Applications Conference. IEEE 2003, p. 632.
15. Kagal, L., Finin, T., and Joshi, A., A Policy Based Approach to Security for the Semantic Web. In 2nd International Semantic Web Conference (ISWC2003), September 2003.
16. Scilla, F., and M. N. Huhns. "Making Agents Secure on the Semantic Web." IEEE Internet Computing (2002): 76-93.
17. Medic, A. & Golubovic, A., Making secure Semantic Web, Universal Journal of Computer Science and Engineering Technology, Vol. 1 No. 2, pp. 99-104. (2010)
18. Chelli, K., Security Issues in Wireless Sensor Networks: Attacks and Countermeasures, Proceedings of the World Congress on Engineering 2015 Vol I WCE 2015, July 1 - 3, 2015, London, U.K.