A Classification Platform for Security Protocols in WSNs

Eliana Stavrou *estavrou@uclan.ac.uk*
University of Central Lancashire, Applied Cyber Security Research Lab
Larnaca, Cyprus

Nearchos Paspallis *npaspallis@uclan.ac.uk*
University of Central Lancashire
Larnaca, Cyprus

Abstract

Wireless Sensor Networks (WSNs) are supporting the operation of a variety of critical infrastructures. In order to secure the operation of WSNs, appropriate security protocols have been specified supporting different operational objectives and security features. Often, it is challenging to identify the protocols' key operation and key features due to various reasons such as the lack of expert knowledge and the complexity of protocols. This can limit the ability of researchers to identify protocols of interest and apply them at a specific setup. This challenge is addressed by designing a platform to classify a wide-range of security protocols in WSNs, to highlight their key features and to guide users through an interactive and user-friendly approach to select protocols of interest. An appropriate proof-of-concept has been developed.
Keywords: protocol classification, security, WSN, decision-tree.

1. Introduction

Wireless Sensor Networks (WSNs) are utilized in a variety of critical infrastructures [2], [9] such as healthcare, smart grid, military, disaster and relief, etc., where operations and data need to be protected. The cyber threat landscape has considerably increased the last few years [1], [7], risking the reliable operation of WSNs. A lot of efforts have been made by the research community to protect WSNs and a number of security protocols have been proposed, covering prevention, e.g. [6], [10], intrusion detection, e.g. [3], [8], and intrusion recovery, e.g. [20-21], aspects. Each of the proposed security protocols promotes specific security features while supporting certain security requirements, e.g. availability, reliability, confidentiality, integrity, etc.

The design and/or application of security protocols in WSNs is not a trivial procedure. Security is a complex field and expert knowledge is often required to design and/or implement an appropriate security protocol in WSNs that will meet specific operational objectives. Often, due to the lack of knowledge, the lack of documentation and the complexity of security mechanisms, it is challenging to design new protocols and/or choose among the available security protocols and apply them in a specific setup to protect the data and the network's operation. Currently, not enough work has been performed to assist people designing new or choosing among existing security protocols in WSNs. To address this challenge, it is essential for people to realize the key features of security protocols so they can be taken into consideration during the protocols' design or selection process.

This research work addresses the aforementioned challenge by contributing a platform that targets to highlight and classify representative techniques/configurations that are available in the security domain in WSNs and present them in a user-friendly way. The platform is envisioned to be utilized by people that: a) have designed secure protocols and will assist them to identify, classify and present the key aspects of their protocol design, b) are designing new secure protocols and need to be aware of existing approaches, and c) need

assistance to choose among existing solutions, the ones that are appropriate for securing their infrastructure.

The remainder of this paper is structured as follows. Section 2 presents related work in the context of secure protocols in WSNs, information provisioning platforms and semantic web technologies. Section 3 discusses the platform's conceptual operation and use cases and section 4 briefly analyzes the corresponding requirements. Section 5 presents the platform's architecture and section 6 illustrates a proof-of-concept. Finally, section 7 summarizes with conclusions and future work.

2. Background work

This section presents background work with regards to the main concepts relevant to this research work.

2.1. Classification of security protocols in WSNs

A large number of secure protocols in WSNs are currently proposed, supporting different security features and security requirements. Typically, security protocols in WSNs fall under the prevention, intrusion detection or intrusion recovery area. Often, identifying the protocols' key operation and functionality is challenging due to various reasons such as lack of expert knowledge, complexity of protocols' operation, etc. The fact that researchers may have difficulties realizing in an easy way the main features of security protocols creates a barrier with regards to identifying protocols of interest. This issue can be addressed by classifying protocols and highlighting their main features.

A variety of state-of-the-art reviews exist today that analyze security protocols in WSNs against different aspects and criteria. Note that this section is not meant to be an exhaustive evaluation comparison of the state-of-the-art reviews. The aim of this section is to highlight that the analysis and classification provided by the state-of-the-art reviews happen at different levels. Some authors discuss and classify protocols under broad categories while others offer a more detailed analysis and categorization. For example, authors in [14] provide a brief review of attacks and corresponding security mechanisms in WSNs. They specify a high-level classification of a broad range of security mechanisms such as secure routing, intrusion detection, privacy, etc., but they do not highlight key features of the listed mechanisms. Wang et al. [22] have performed an extensive survey of security issues in WSNs and have categorized protocols based on their operation at specific layers of the protocol stack. Authors in [19] have also contributed an extensive review, focusing on multipath routing protocols in WSNs. They have identified the key operation of protocols and categorized them based on their operational objectives and supported security requirements. A number of surveys have been performed in the context of intrusion detection area in WSNs. Authors in [12] have classified protocols based on six criteria: target system, detection technique, collection process, trust model, analysis technique and response strategy. Singh et al. [18] have categorized intrusion detection protocols in WSNs taking into consideration the detection technique that is implemented. A similar approach is taken by [15] with the difference that authors provide an extensive analysis of the different intrusion detection schemes.

Although state-of-the-art reviews promote classification of security protocols in WSNs, they are not adequate. Classification needs to be contacted in a uniform and guided way that will allow researchers to: a) add new protocols that can be classified under the existing classification schemes, b) easily extend the existing classifications to include new security features, and c) seek protocols that support a specific set of security features. For such a classification scheme to be efficient and effective, an appropriate system is required so that context related to the protocols can be provided, maintained, retrieved and presented to interested users. To the best of our knowledge, such a system does not yet exist.

2.2. Semantic web technologies

Security is a critical aspect of modern computing infrastructures, yet the selection of the most appropriate tools and configurations remains a daunting task. As argued by Ion et al. [5], "*Too many things are asked of them* [the users], *which may be unrealistic, time consuming, or not really worth the effort.*" As a result, assisting or even automating this task—commonly via an information provisioning platform—has seen increased interest in recent years.

On one hand, basic recommender systems have been exploited for years but are commonly limited to scenarios where the input size is significant and be used for supervised learning of the underlying system (e.g. recommending books, movies, etc.) [16].

The Web has been one of the most successful technologies of the last decades. It is no surprise then that a lot of effort has been focused on the development of websites. An overview of the main trends in Web application development are discussed in [6] and include the Client-server paradigm, Caching, the AJAX paradigm (Asynchronous JavaScript and XML), Thin- and Fat-client computing, etc.

Dynamic website creation is now**a**days a popular trend. The authors of a relevant work, proposed an execution-based model as "a *continuous process to improve prescriptive models at design-time through runtime information by incorporating knowledge in form of profiled metadata from event logs generated during the execution of a code model*" [11]. Towards this goal, these authors proposed a blend of techniques originally conceived for Process Mining with methods used to develop Runtime models of Model Driven Development.

3. Platform conceptual operation

The aim of the platform is to provide the means to people to highlight the operation of their security protocols in WSNs, to make the information available to a platform in a uniform way for visualization purposes and to assist users realizing security techniques and choosing potential security protocols of interest. Different aspects need to be investigated and specified in order to design and implement such a platform. An appropriate conceptual architecture is proposed to aid the design and implementation efforts and support the platform's objectives.

3.1. Conceptual operation

Figure 1 presents an overview of how this platform is envisioned conceptually.

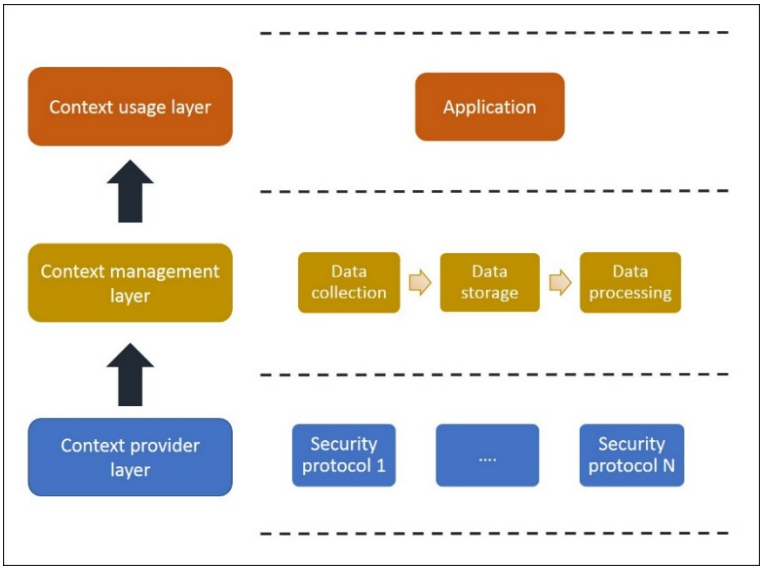

Fig. 1. Platform conceptual operation

As indicated in Figure 1, the platform consists of 3 layers:

- Context provider layer. Users are expected to provide data to the platform with regards to security protocols in WSNs. These users are considered experts in the field of security that can identify the key operation and features of the protocols.
- Context management layer. This layer is concerned with the data management. Specifically, the key tasks of this layer include:
    - Data collection. The platform will provide the means for data acquisition by the user in a uniform way. To accomplish this, an appropriate semantic/conceptual data model will be specified to allow the user to break-down and highlight the protocols' key operation and features. Data validation will be performed in order to verify that the data provided by the users comply with the data modeling rules.
    - Data storage. The operation of the platform will be supported by an appropriate database that will store context related to the security protocols in WSNs, users' information, etc.
    - Data processing. The platform will process the instance data of the semantic data model and interpret them appropriately to facilitate visualization purposes and promote the platform's objectives.
- Context usage layer. This layer concerns the application that will consume the instance data of the semantic data model and visualize them in a user-friendly way that will highlight the key operation of the underlying security protocols in WSNs represented by the data model.

3.2. Conceptual classification model

A key element of the platform is data modelling to facilitate protocol classification. As specified earlier, an appropriate semantic data model will be specified to guide the users to identify and classify the main features of their protocols. This model will be also utilized for visualization purposes in order to assist users identifying security protocols in WSNs that support a specific set of security features.

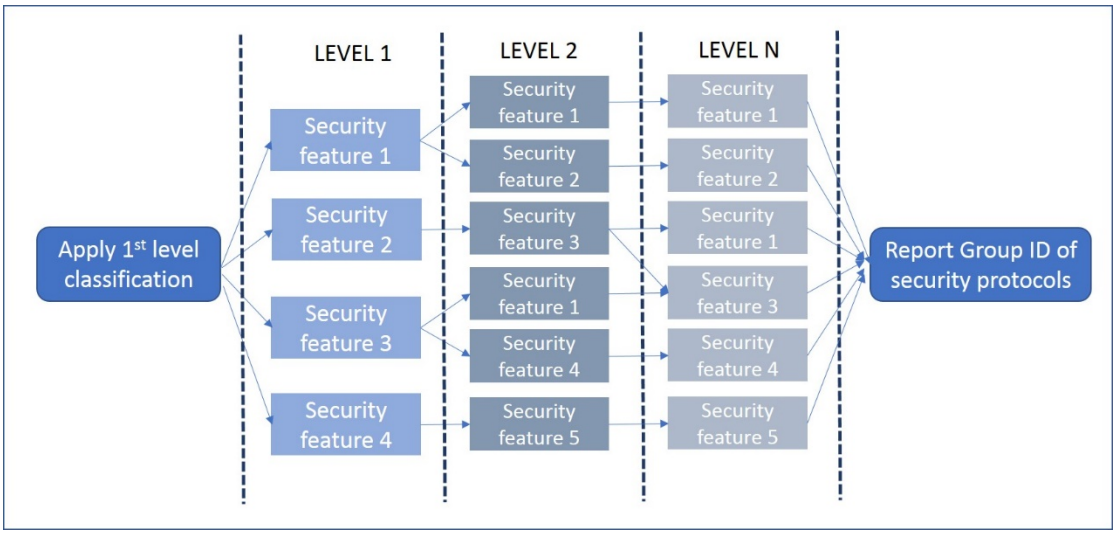

Fig. 2. Platform conceptual classification model

The platform utilizes a hierarchical data model to promote the efficient analysis, classification and visualization of complex data. Hierarchical models utilize a decision-tree approach where the analysis/classification in one step is guided by the previous step. This approach will allow the users of the platform to arrive at a result which can represent a single or a set of protocols that utilize common security features. Figure 2 presents a conceptual workflow of the hierarchical model utilized by the platform. As depicted in Figure 2, a

number of classification levels can be defined, each level representing a unique security feature of the underlying set of security protocols. At the end, a group of security protocols will be recommended based on the classification path followed by the user. For each classification made at level 1, a new instance of the data model will be specified. Each instance of the data model represents a unique path that corresponds to a specific classification which begins with a key feature at level 1. This allows the platform to integrate new classifications of security protocols that have not been considered during the initial development of the platform.

3.3. Use case scenarios

Following, the key use case scenarios supported by the platform are briefly discussed.

a) Context provisioning
Figure 3 presents the use case scenario with regards to context provisioning. Expert users, e.g. protocol designers, are expected to break-down the operation of their security protocols and utilize the platform's data model in order to allow the platform to classify the underlying protocols. The platform will allow expert users to extend an existing instance of the data model by adding new classification levels and/or update it to include their protocol under the specified data model. The former case will occur if the protocols to be classified support new security features that are not currently classified by the data model under consideration. Moreover, the platform will allow the users to create new instances of the data model in the case where their protocol cannot be classified under any of the features in level 1. In this case, the platform will create a new element in level 1, representing a feature that is not currently included. Once the user extends an existing one or creates a new instance of the data model, he/she has to make it available to the platform. The platform will have to validate that the data model instance complies to the data modelling rules in order to push it to the corresponding application that will be responsible to visualize the classification of the protocols. In the case that the provided data instance is not validated, the user will be prompt to correct it appropriately.

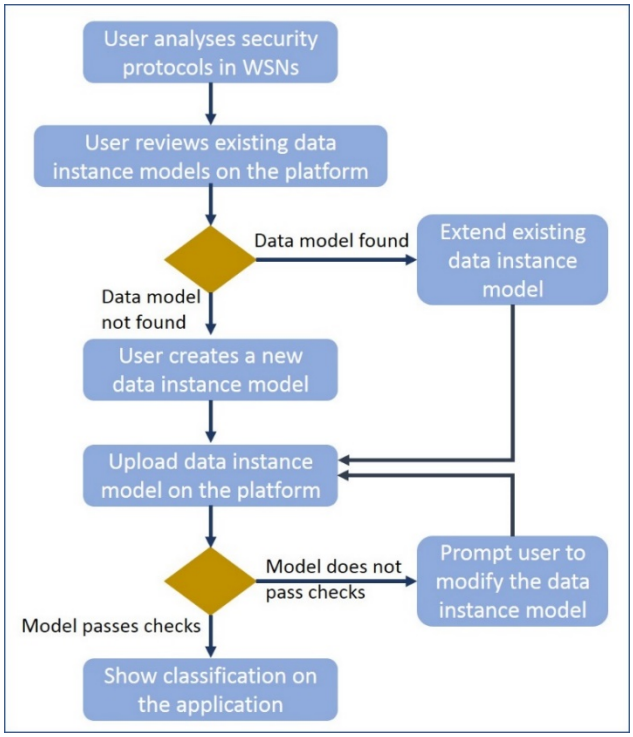

Fig. 3. Context provisioning use case scenario

b) Selection of security protocols in WSNs

Figure 4 illustrates how users can utilize the platform to realize the security techniques and features that are supported by security protocols in WSNs and choose the ones that are of interest. As discussed in Section 3.2, the platform utilizes a decision-tree approach to classify and visualize protocols. This means that a variety of logic statements will be presented to the user at each classification level. The user will be expected to make a decision (select among a set of existing answers) in order to move on to the next classification level. At the end of the tree, a set of protocols will be presented to the user. The recommended protocols are the ones that support the features that have been previously selected by the user. At this stage, the platform will provide further information to the users with regards to each recommended protocol such as publication source and venue, authors, detailed description, etc.

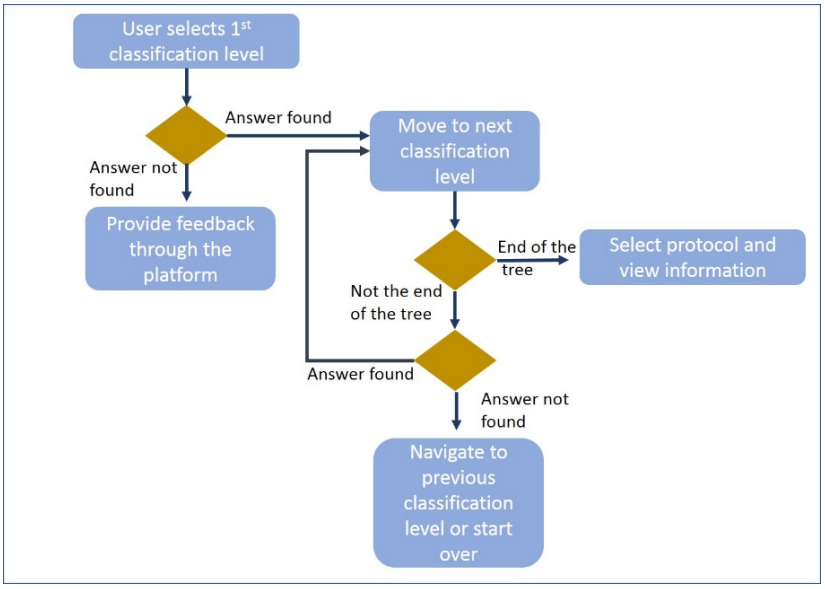

Fig. 4. Selection of security protocols in WSNs use case scenario

4. Platform key requirements

Based on the conceptual architecture discussed in Section 3.1 and the use cases presented in Section 3.3, a set of key requirements have been specified. The key requirements will drive the platform's design which is presented in Section 5.

- Extensibility

The platform should allow the users to extend existing classifications with new security features and/or create new ones. Such a behavior will promote the future growth of the platform and also increase the platform's added value.

- Dynamic content modifiability

The previous requirement can support the dynamic modifiability of the specified protocol classifications without impacting the overall architecture of the platform, or at least having a minimum impact on specific parts of the platform. Such an ability can also support a dynamic visualization of the protocols' classification levels.

- Interactive protocol selection

The platform needs to support an interactive behavior in order to promote a user-friendly approach with regards to selecting protocols of interest. As previously discussed, a decision-tree approach will be utilized to visualize the protocols' classification. By allowing the users to interact with the decision-tree, they will be able to easily navigate through the tree, identifying security features (and eventually security protocols) of interest.

- Usability

It is important for the platform to be usable and allow the users to easily interact with it in order to select security features and protocols of interest. Usability is a key requirement to achieve users' satisfaction and utilization of the platform.

- Generic data input model

The platform needs to incorporate a generic data input model in order to be able to classify a wide range of security protocols that exist in WSNs, without been limited by the capabilities of certain protocols.

- User friendly

It is critical to promote the specification of a generic data input model that can be easily understood by designers and utilized to classify their protocols on the platform. Such a user-friendly model should also allow designers and/or the platform to cross-check its correctness.

5. Architecture

This section presents the main components and key functionality of the architecture with regards to data representation, storage, visualization, etc. Mainly, the platform allows the specification of an interactive flow through a model, and its interpretation by a system which realizes the flow based on user input. This section presents the core elements of the architecture, namely the model used to specify the classification of the WSN protocols, and the logic needed to realize the interactive sessions for the selection of the most appropriate protocol.

5.1. Protocol selection model

For the purposes of enabling maximum flexibility, we have defined a JSON-encoded schema which allows the designers to quickly specify a selection protocol in a user-friendly way. JSON (*JavaScript Object Notation*) was selected as it is a lightweight data-interchange format which is easy for humans to read and write. Furthermore, it is based on a subset of the JavaScript Programming Language and thus the latter has full support for it [13], [17].

The schema specifies the individual protocols (or families of protocols) through an ID, a short description, and optionally a URL providing further details. The interactive selection logic is realized through a simple set of rules, each of which specifies a question, and an arbitrary number of answers (i.e. selections), with their corresponding action. Each question must specify one or more answers, and each answer is linked to an action (which can be either another question or a protocol selection). For instance, the protocol classification illustrated in Figure 6 can be modeled through this as follows:

```
{
  "protocols": [
    { "id": "p1", "name": "Group 1 protocols",
      "description": "Protocols focusing on prevention",
      "url": "http://..."},
    {"id": "p2", "name": "Group 2 protocols",
      "description": "Protocols focusing on intrusion detection",
      "url": "http://...."},
    {"id": "p3", "name": "Group 3 protocols",
      "description": "Protocols for high level security",
      "url": "http://...."},
    {"id": "p4", "name": "Group 4 protocols",
      "description": "Protocols for low level security",
      "url": "http://...."}
   ],
```

```
  "logic": [
    { "id": "q0", "question": "Choose a technique to promote reliable
      communication",
      "answers": [
        { "Multipath routing": "q1" },
        { "Acknowledgements (ACK) utilized": "q2"} ]},
    { "id": "q1",
      "question": "Choose a technique",
      "answers": [
        { "Prevention": "p1" },
        { "Intrusion detection": "p2"} ]},
    { "id": "q2",
      "question": "What is your targeted security level?",
      "answers": [
        { "High": "q21" },
        { "Low": "q22"} ]},
    { "id": "q21",
      "question": "Choose an ACK technique",
      "answers": [
        { "Select": "p3" } ]},
    { "id": "q22",
      "question": "Choose an ACK technique",
      "answers": [
        { "Select": "p4" } ]}
  ]
}
```

Notably, the model builds on an (inverted) tree-based structure, where the root is the starting point, and the leaves are the possible selections. Branches in the tree are decision points, where user interaction is requested. There are no blind paths (i.e. all leaves are endpoints indicating a decision).

5.2. Conceptual platform architecture and implementation

The conceptual architecture of the system is illustrated in Figure 5. The main actors are the users (using the interactive system to identify an appropriate protocol by iterating a sequence of questions and answers), and the model designers who specify and store the corresponding protocol selection models in the system. An appropriate authentication mechanism (not illustrated) is necessary to ensure proper use and non-corruption of the system.

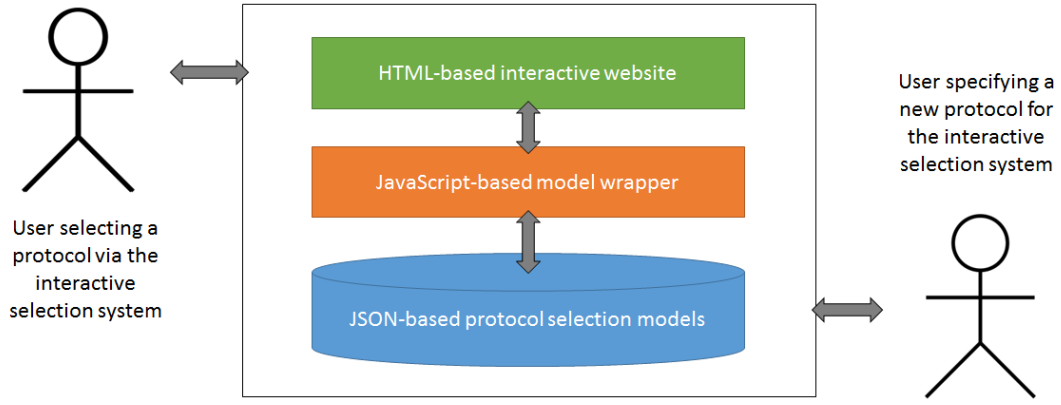

Fig. 5. Conceptual architecture of the protocol selection system

Once a user selects a specific model, the JavaScript-based model wrapper takes over and interprets the model as a dynamic, interactive website. Based on the individual protocols, and

the selection logic, the JavaScript wrapper dynamically edits the HTML-based page to display the corresponding questions along with the answers. Any optional URLs are automatically converted to anchor links opening to external websites. Examples of the resulting views are presented in Figures 7, 8 and 9.

6. Proof-of-concept

In order to provide a proof-of-concept, the following tasks have been realized:

a) Decide of the level 1 (root) classification criteria.
b) Analyze a set of protocols and identify their key security features.
c) Create a paper-based decision-tree structure with logic statements that will allow of the protocols features' classification. The logic statements should allow the users to progress from one level to the next classification level.
d) Model the structure created at the previous task using the data model described at Section 5 and considering the relevant modelling rules.
e) Upload the data model on the platform.
f) Provide details through the platform with regards to each protocol that is classified under the provided data model.
g) Navigate to the application to visualize the new classification.

With regards to point a, it has been considered that, typically, security protocols promote a primary security requirement. Therefore, it has been decided that protocols will be classified at level 1 as per the security requirement they are promoting e.g. reliability, availability, confidentiality, integrity, etc. With regards to point b, it needs to be stated that a number of security protocols in WSNs have been proposed in the last few years. Initially, we have decided to classify protocols that promote reliability and considered a survey of secure multipath routing protocols in WSNs [19]. Then, the decision-tree structure has been specified as indicated in Figure 6 which served as the basis for the corresponding data model.

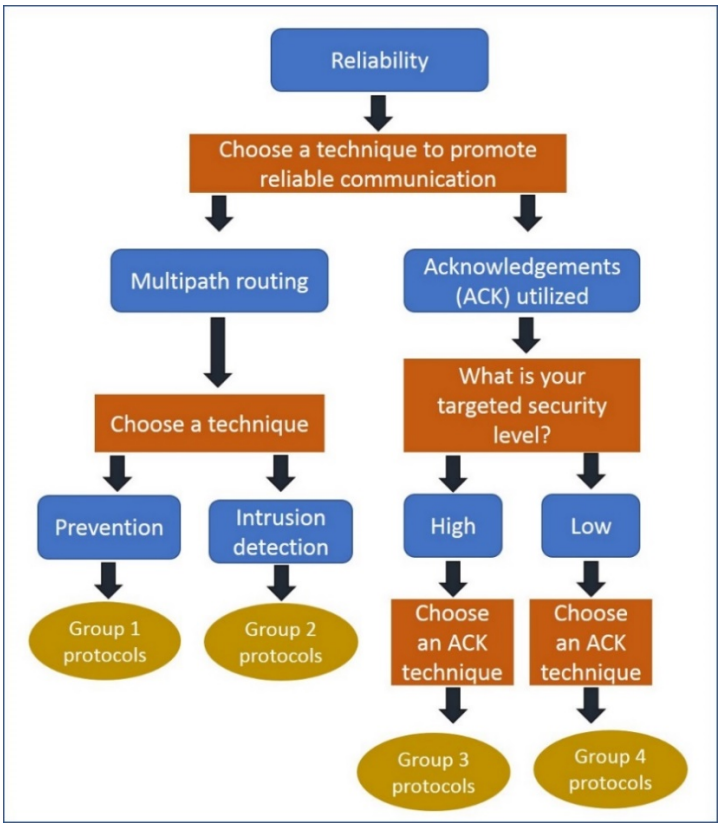

Fig. 6. Decision-tree structure for reliability classification

As discussed in Section 5, an appropriate web site has been designed to promote the objectives of this work and present the classification of security protocols in WSNs. Figures 7, 8 and 9 illustrate how the decision tree is presented on the web site. The web site is divided into two areas. At the right-side area, all protocols under reliability criterion are listed. At the left-side area, the user is presented with specific logic statements/questions to guide him/her on the choices that can be made. The user navigates to the decision-tree depending on the choices made and at the end the web site presents the recommended protocols. At the end, by selecting a specific protocol, further information is presented to the user.

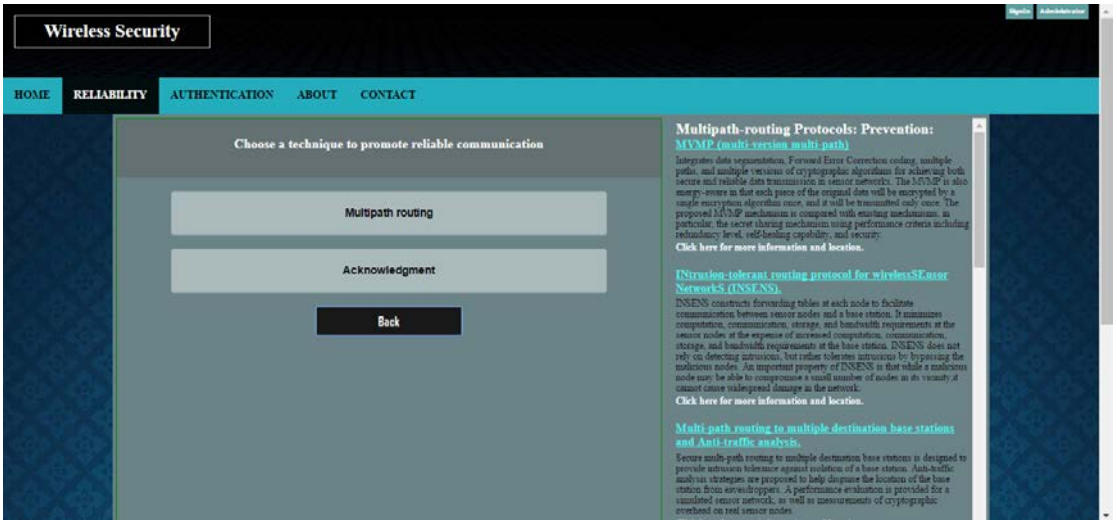

Fig. 7. First level classification example

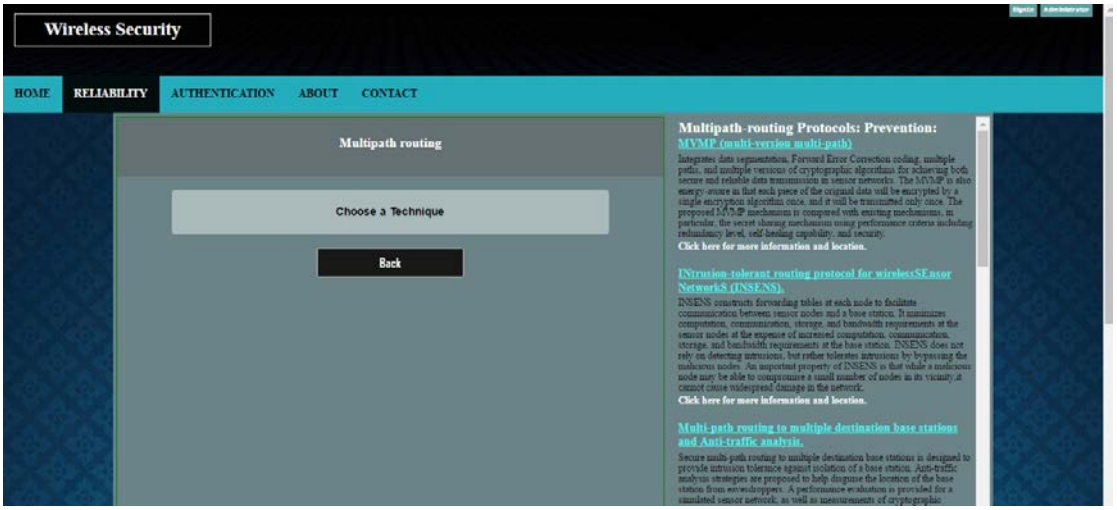

Fig. 8. Second level classification example

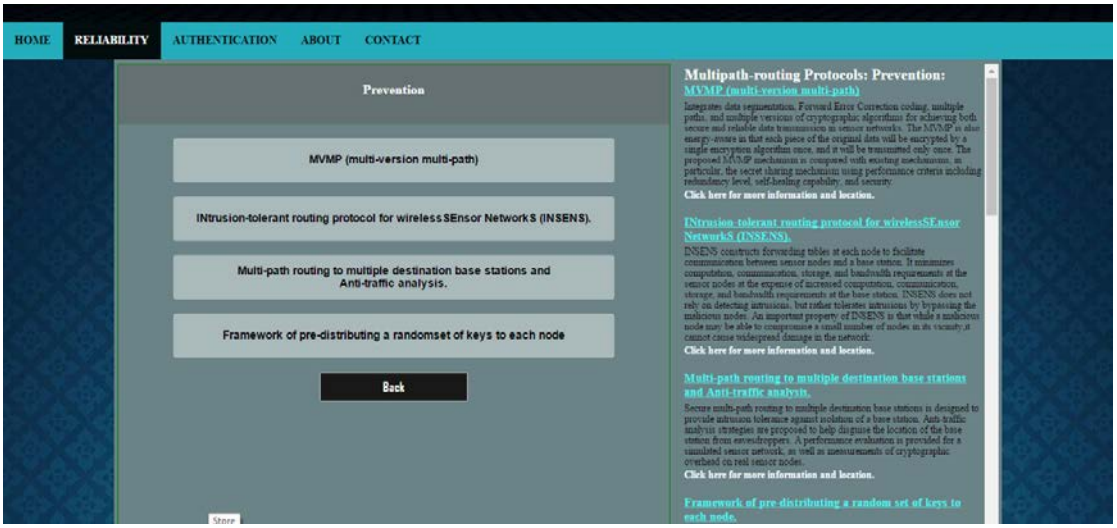

Fig. 9. Third level classification example

7. Conclusions

Security is an essential feature that is required to protect the operation of WSNs, especially in the case where they support critical infrastructures. Usually, expert knowledge is required to realize the security aspects that need to be considered in WSNs. If such knowledge is not present, it may be challenging to design security protocols in WSNs and/or select protocols among a large pool of existing ones. To address this challenge, a new platform has been designed to allow users to classify and list their security protocols, highlighting the protocols' key operation and security features. Moreover, the platform guides users through an interactive approach to realize and select security features and protocols of interest that can be implemented to promote certain operational objectives. At the end, a proof-of-concept has been demonstrated. As future work, we plan to enhance the platform by including more security protocols and features.

Acknowledgements

The authors would like to thank Petronila Midala that has implemented the proof-of-concept as part of her B.Sc. thesis project.

References

1. ENISA Threat Landscape (2014), https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014. Accessed April 28, 2017.
2. Garcia-Hernandez, C. F., Ibarguengoytia-Gonzalez, P. H., Garcia-Hernandez, J, Perez-Diaz, J. A.: Wireless sensor networks and application: a survey, International Journal of Computer Science and Network Security (IJCSNS), 7 (3), pp. 264-273 (2007)
3. Hegazy, I., Safavi-Naini, R., Williamson, C.: Towards securing MintRoute in wireless sensor networks, IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM), Montreal, QC, Canada, pp. 1-6 (2010)
4. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: Attacks and Countermeasures, In Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113-127 (2003)

5. Ion, I., Reeder, R., Consolvo, S.: "...no one can hack my mind": Comparing Expert and Non-Expert Security Practices, In Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS), Ottawa, Canada (2015)
6. Jazayeri, M.: Some Trends in Web Application Development. In Future of Software Engineering (FOSE), IEEE Computer Society, Washington, DC, USA, pp. 199-213 (2007)
7. Klahr, R., Shah, J. N., Sheriffs, P., Rossington, T., Pestell, G.: Cyber Security Breaches Survey 2017, https://www.ipsos-mori.com/Assets/Docs/Publications/sri-cybersecurity-breaches-survey-2017.pdf. Accessed April 28, 2017.
8. Krontiris, I., Benenson, Z., Giannetsos, T., Freiling, F. C., Dimitriou, T.: Cooperative intrusion detection in wireless sensor networks, In Proceedings of the 6th European Conference on Wireless Sensor Networks, Berlin, Heidelberg, Springer-Verlag, pp. 263-278 (2009)
9. Kuorilehto, M., Hännikäinen, M., Hännikäinen, T. D.: A survey of application distribution in wireless sensor networks, EURASIP Journal of Wireless Comm. and Networking, 4, pp. 774-788 (2005)
10. Lee, S., Choi, Y.: A secure alternate path routing in sensor networks, Computer Communications, Elsevier, 30 (1), pp. 153-165 (2006)
11. Mazak, A., Wimmer, M.: On Marrying Model-driven Engineering and Process Mining: A Case Study in Execution-based Model Profiling, Vortrag: 6th IFIP International Symposium on Data-Driven Process Discovery and Analysis (SIMPDA 2016), Graz, pp. 1–10 (2016)
12. Mitchel, R., Chen, I-R.: A survey of intrusion detection in wireless network applications, Journal of Computer Communications, Elsevier, 42, pp. 1-23 (2014)
13. Nolan, D., Lang, D. T.: JavaScript Object Notation, Chapter 7 in XML and Web Technologies for Data Sciences with R, Springer, pp. 227-253 (2013)
14. Padmavathi, G., Shanmugapriya, D.: A survey of attacks, security mechanisms and challenges in wireless sensor networks, International Journal of Computer Science and Information Security (IJCSIS), 4 (1 & 2) (2009)
15. Rassam, M.A., Maarof, M.A., Zainal, A.: A survey of intrusion detection schemes in wireless sensor networks, American Journal of Applied Sciences, 9 (10), pp. 1636-1652 (2012)
16. Ricci, F., Rokach, L., Shapira, B., Kantor, P. B.: Recommender Systems Handbook, Springer, Boston, Massachussets, USA (2011)
17. Severance, C., "Discovering JavaScript Object Notation," in Computer, vol. 45, no. 4, pp. 6-8, April 2012. doi: 10.1109/MC.2012.132
18. Singh, M., Babbar, K., Lata Jain, K.: A Survey on Intrusion Detection System in Wireless Sensor Networks, International Journal of Wireless Communications and Networking Technologies, 3 (3) (2014)
19. Stavrou, E., Pitsillides, A.: A survey on secure multipath routing protocols in WSNs, Computer Networks Journal (COMNET), 54 (13) (2010)
20. Stavrou, E., Pitsillides, A.: Combating persistent adversaries in wireless sensor networks using directional antennas, 18th International Conference on Telecommunications (ICT), Ayia Napa, Cyprus, pp. 433-438 (2011)
21. Stavrou, E., Pitsillides, A.: WSN operability during persistent attack execution, 23rd International Conference on Telecommunications (ICT), 16-18 May 2016, Thessaloniki, Greece, pp. 1-5 (2016)
22. Wang, Y., Attebury, G., Ramamurthy, B.: A survey of security issues in wireless sensor networks, IEEE Communications Surveys & Tutorials, 8 (2), pp. 2–23 (2006)