# A FORMAL MODEL PROPOSAL FOR WIRELESS NETWORK SECURITY PROTOCOLS

**Shabir Ahmad*[1], Shafiq Hussain[2], Khalid Khurshid[3]**
[1]Government College of Commerce, Multan
*Email: mian_shabbir@hotmail.com (Corresponding Author)
[2]Department of Computer Science, Bahauddin Zakariya University, Sub-Campus Sahiwal, Pakistan
[3]Department of Education, Bahauddin Zakariya University, Multan.

***ABSTRACT--****With the exploding growth on wireless communication in recent years, security issues in wireless networks also become a growing concern. Traditionally, the main method for analyzing wireless networks protocols is simulation. However, the development of adequate formalisms for modeling and analysis of wireless networks has not kept pace with this. Formal method is a way to takes the specification (written in natural language) and converts it into its mathematical equivalent. Formal methods may also be useful for proving properties on the specified models. These proofs could be performed automatically, using model checkers, or interactively through proof tools. Event-B is a formal specification language used to specify formal models of a system under study. Rodin is a tool and development system for the specification, verification and validation of formal models of the software systems. In the proposed methodology, our main objective is to formally specify, analyze, verify and validate the wireless protected access version-2 (WPA2) security protocol. The purpose of this research is to develop a framework for the use of formal methods in the specification, verification and validation of wireless network security protocols. The benefit of this formal framework allows wireless network users to exchange data and information between wireless devices and cell phones reliably.*

**KEYWORDS:** Wireless Networks, Security Protocols, Formal Methods, Event-B, Rodin, Verification, WPA2.

## 1. INTRODUCTION

With the exploding growth on wireless communication in recent years, security issues in wireless networks also become a growing concern. Security requirements for wireless networks are similar to those for wired networks. However, wireless networks are inherently less secure compared to their wired counterparts due to the lack of physical infrastructure. Therefore, special attention should be paid to the security of wireless networks. The security objectives for wireless and wired networks are the same, as are the major high-level categories of threats that they face. However, while these objectives are well understood and addressed in the relatively mature wired network environment this has not always been the case in the new and rapidly evolving wireless environment. Different wireless security protocols were created to ensure home wireless networks. These wireless security protocols incorporate WEP, WPA, WPA2, Zigbee, Pkmv1 and Pkmv2 each with their own particular qualities and shortcomings. Formal tools are used to describe the security properties and perform efficient verification of protocol's correctness properties. Issues like inconsistencies and incompleteness always remain there if there is no proper analysis of protocols properties. Formal methods are tools and techniques based on mathematical logic. Formal methods are used for the specification, verification and validation of software as well as hardware systems. Formal method will also bring to light all different probable perspective to any given variables and functions that could have been hidden behind the English language. This can be done using a number of formal languages such as Z notation, VDM, Algebra etc. Formal methods can be used for analysis and specification of systems. Model based specifications, as well as declarative and algebraic specifications, fit under this category. Formal methods may also be useful for proving properties on the specified models. Formal methods have been used to specify security protocols and verify security properties, such as confidentiality, authentication and non-repudiation to guarantee correctness.

## 2. BACKGROUND

Many traditional models for the analysis of wireless network security protocols have developed. S. Andova et al. [1], have developed a framework to analysis many security protocols. The framework is capable to perform automatic as well as manual verification of complex security protocols. The approach is used to verify protocols properties to illustrate the applicability of the framework to real-world protocols. Traditionally, the main method for analyzing wireless networks protocols is simulation. There are several established tools for the simulation of wireless networks protocols, including ns-2 [2], OPNeT Modeler [3] and GloMoSim [4]. Many case studies demonstrate the use of simulation methods [5, 6, 7]. Similar observations are made by Kotz et al. [8], who criticize the use of oversimplified assumptions in the radio models of many simulators, a lack of empirical validation, and incorrect abstractions of network layers. Demaille et al. [9] use the approximate verification tool APMC [10] to analyze a wireless sensor network for intrusion detection. They consider LTL properties for discrete-time probabilistic models of 100 and 400 nodes.

In recent years, wireless networking has enjoyed a great and steadily growing popularity in both research and industry. However, the development of adequate formalisms for modeling and analysis of wireless networks has not kept pace with this, with Chalmers et al. in the Grand Challenges for Computing Research [11] stating a "considerable lack of formal foundations". Model checking is an algorithmic approach to exhaustively and automatically establish system properties. Probabilistic model checking, in particular the probabilistic model checker PRISM [12], has been successfully employed for the verification of various network protocols. These include: IEEE 802.11 WLAN contention resolution [13], IEEE 1394 FireWire root contention [14], and Bluetooth device discovery [15]. Kwiatkowska et al. [16] give an overview about different types of probabilistic temporal-logic properties of wireless network protocols that can be analyzed using PRISM. To the best of our knowledge, CaVi [17] is the only tool that provides a uniform interface for formal analysis and simulation of wireless sensor networks and it is the only tool that incorporates realistic wireless channel or radio models into model checking. Seada et al. [18] mention the problem of finding sensible topologies when designing wireless sensor networks that is, adjusting channel and radio parameters values in order to achieve good reception probabilities. Bo Han, Weijia Jia, Lidong Lin [19] proposes a collision-free centralized scheduling algorithm for IEEE 802.16. Cremers, C. J. [20], made a formal analysis of authentication protocol IEEE 802.16 WiMAX (PKMv1 and PKMv2) and proposed a new protocol more reliable. The Scyther tool, which provides formal proofs of the security protocol is used as model checker. Sen Xu, Chin-Tser Huang, Manton M. Matthews [21], models the PKM protocols using Casper and analyzes the CSP output with FDR, which are formal analysis tools based on the model checker. Later versions of PKM protocols are also modeled and analyzed. Beth N. Komu, Mjumo Mzyece and Karim Djouani [22], analyse a security protocol proposed to mitigate the MITM attack at the initial network entry point in WiMAX referred to as Secure Initial Network Entry Protocol (SINEP), and model the protocol and an intruder process with MITM capabilities in Process/Protocol Meta-language (PROMELA) formalism. Researchers then use Linear Temporal Logic (LTL) to define the attributes the protocol should satisfy and carry out verification by use of the SPIN model checker. A Real-Time Maude language and tool can be used to formally model, simulate, and model check advanced wireless sensor network (WSN) algorithms [23]. A Event-B formal verification method used to model and verify ZigBee protocol stack by providing embedding of the protocol primitives in Event-B [24]. The approach takes advantage of the Event-B method capabilities to model designs at different levels of abstraction which fits the layered nature of the protocol.

## 3. FORMAL METHODS

Clarke &Wing in 1996 [25] described formal specification languages and analysis tools as the two main reasons of using formal methods in software development. They discussed that informal and semi-formal techniques of software development are not sufficient to develop reliable systems due to the complex nature of software systems and issues related to these approaches. The first issue of informal and semi-formal techniques is the natural language in which software systems are specified. The words and sentences in natural languages can be interpreted as having to multiple meanings. These words have specific meanings within s specific context. Therefore, the issues like ambiguities, incompleteness and contradictions are always present in the systems specified by using natural languages. The second issue is the lack of automatic or semi-automatic tools for the analysis of specifications written in natural language. In the following paragraphs, we will describe the benefits of using formal methods in the development of software systems. Clarke & Wing argue that formal methods help to produce accurate and precise specifications of software systems. Since formal methods use mathematical logic for the specification of software systems, the resulting specifications are free of ambiguities, incompleteness and contradictions. It helps to identify errors and issues at the specification and design level. The use of formal methods also increases the understanding of designer in the system. Hence, better designs for software systems can be developed. Formal method is a way to takes the specification (written in natural language) and converts it into its mathematical equivalent. Thus it is normally used in the SDLC Analysis and Design stages. The natural language usually contains ambiguous, incomplete and inconsistent statement. Once a specification in English for example is translated to a mathematical form, it will remove all ambiguity and uncertainty in that statement. Formal methods may also be useful for proving properties on the specified models. These proofs could be performed automatically, using model checkers, or interactively through proof tools. Formal specification and security analysis have a long research history in computer science, as for the development of network protocols. Figure 1 illustrates the procedure of the formal approach.

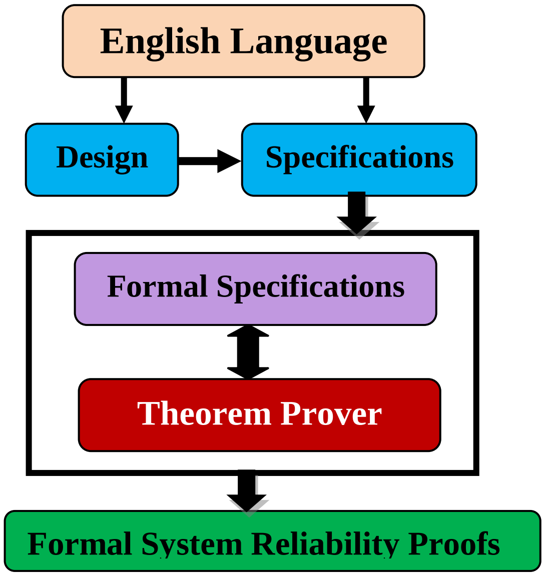


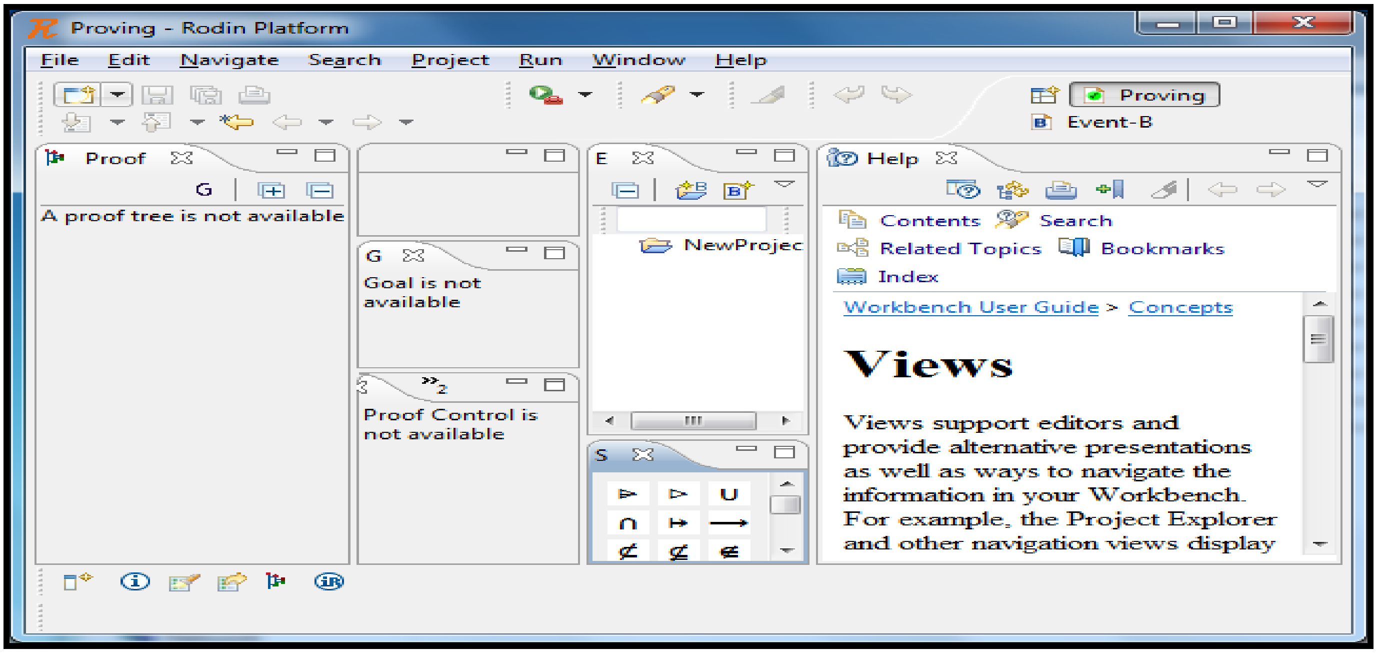
**Figure 1: Formal Approach Procedure**

### 3.1 Event-B

Event-B is a formal specification language used to specify formal models of a system under study. This language is based on set theory and has a lot of tool support. The use of set theory in Event-B is its key feature. Event-B is developed by Jean-Raymond Abrial and is an evolution of B-Method [26, 27]. Models developed in Event-B can be verified by using theorem provers, checked by using model checker and validated by using automated validation tools such as AnimB. The use of Event-B provides a rich expressive modeling language, and on the other hand, it is less interactive, compared to HOL theorem proving approach. System and Software Engineering provides a comprehensive exposition of the Event-B approach for modelling and reasoning.

### 3.2 RODIN Tools

Rodin is a tool and development system for the specification, verification and validation of formal models of the software systems. Rodin stands for Rigorous Open Development Environment for complex systems. This is a latest formal method tool developed in 2009 under the European Union



A proof tree is not available

Goal is not available

Proof Control is not available

Views

Views support editors and provide alternative presentations as well as ways to navigate the information in your Workbench. For example, the Project Explorer and other navigation views display

Figure 2: IDE of Rodin

Project Deploy. The development of Rodin makes the formal development of software very easy. There are a number of integrated tools in the Rodin platform including theorem provers and model checkers. The Rodin Platform is an Eclipse-based IDE for Event-B that provides effective support for refinement and mathematical proof [28].

## 4. THE PROPOSED METHODOLOGY

In the proposed methodology, our main objective is to formally specify, analyze, verify and validate the WPA2 security protocol. The major phases of this methodology are as under:

### 4.1 Development of Framework

The purpose of this research is to develop a framework for the use of formal methods in the specification, verification and validation of wireless network security protocols. Formal methods are the rigorous mathematical approaches for modeling and designing complex systems. These approaches have a number of applications in the design of systems such NASA projects; Nuclear weapons control systems, complex medical systems and air traffic control systems etc. In this research, we will light weight use of formal methods.

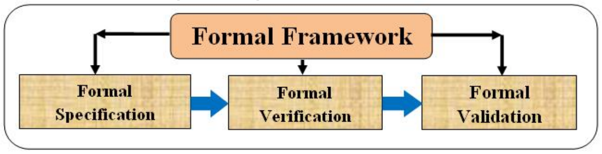


Figure 3: Proposed Formal Framework

### 4.2 Formal Specification

Formal specification is a description of the system under study in a mathematical language such as Z, VDM, B-Methods and Event-B etc. This formal specification consists of all the user requirements written in a clear, unambiguous and systematic way. In this study, we will formally specify WAP2 security protocol in Event-B language which is a formal specification language based on set theory and first order predicate logic. These Event-B specifications will be written using Camile Editor, available as plug-in in the RODIN Tools. These formal specifications will act as formal model of the system.

### 4.3 Formal Verification

Formal verification is the process to ensure the system consistency. It ensures that system is correct and consistent with respect to all the invariants and constraints defined in the system. It also ensures that system is free of all dead locks and race conditions. If all the proof obligations are discharged then the system is said to be verified. Formal verification is the analysis and proof generation process of the formal models of the system which are based on the formal specifications. In formal verification we can prove that the formal models of the system are consistent and there is no loop hole in the system. We can also prove that system is correct with respect to the expectations. In this study, formal verification will be done by using Atelier-B provers and ProB model checker. Since systems in Event-B are developed in layers, therefore, it is necessary to make is ensure that the system is consistent with each layer and refinement.

### 4.4 Formal Validation

Formal validation is the process of proving that system is correct with respect to user requirements. All the user requirements are converted into mathematical formulas. Then these formulas are proved against the formal models of the system. All the user requirements are validated in this way. In this research, formal validation will be done by using AnimB tool. The AnimB tool is an animator and formal validation tool for the validation of Event-B models. This tool is available as a plug-in to RODIN tools.

## 5. RESULTS AND DISCUSSIONS

The benefits of study of formal method for wireless network security protocol, allows wireless network users to exchange data and information between wireless devices and cell phones reliably. With the help of formal model for wireless network security protocols take the advantages like wireless services will be available quicker, reducing cost, giving more security to the network users. Formal model provides benefits like Integration, Interoperability, Agile development, Scalability and Cost Efficient.

## REFERENCES

1. Andova, Suzana, et al. "A framework for compositional verification of security protocols." *Information and Computation* 206.2 (2008): 425-459 (Elsevier).
2. The Network Simulator ns 2. http://www.isi.edu/nsnam/ns/.
3. OPNeT. http://www.opnet.com/.
4. GloMoSim: Global Mobile Information Systems Simulation Library. http://pcl.cs. ucla.edu/projects/glomosim/.
5. Byung-Jae Kwak, Nah-Oak Song, and Leonard E. Miller. Performance analysis of exponential backoff. *IEEE/ACM Transactions on Networking*, 13(2):343–355, 2005.
6. Marcel Neugebauer, Jrn Pl¨onnigs, and Klaus Kabitzsch. A new beacon order adaptation algorithm for IEEE 802.15.4 networks. In *Proceedings of the 2nd European Workshop on Wireless Sensor Networks (EWSN 2005)*, pages 302–311, 2005.
7. Tony Sun, Ling-Jyh Chen, Chih-Chieh Han, Guang Yang, and Mario Gerla. Measuring effective capacity of IEEE 802.15.4 beaconless mode. In *Proceedings of the 2006 IEEE Wireless Communications and Networking Conference (WCNC 2006)*, volume 4, pages 493–498, 2006.
8. David Kotz, Calvin Newport, Robert S. Gray, Jason Liu, Yougu Yuan, and Chip Elliott. Experimental evaluation of wireless. In Proceedings of the 7th ACM International Symposium on Modeling, Analysis and Simulation for Wireless and Mobile Systems (MSWiM 2004), pages 78–82, 2004.
9. Akim Demaille, Thomas H´erault, and Sylvain Peyronnet. Probabilistic verification of sensor networks. In Proceedings of the 14th IEEE International Conference on Computer Sciences, Research, Innovation and Vision for the Future (RIVF 2006), pages 45–54. IEEE Computer Society Press, 2006.
10. APMC: Approximate Probabilistic Model Checker. http://apmc.berbiqui.org/.
11. Dan Chalmers, Matthew Chalmers, Jon Crowcroft, Marta Kwiatkowska, Robin ilner, Eammon O'Neill, Tom Rodden, Vladimiro Sassone, and Morris Sloman. Ubiquitous computing: Experience, design and science, 2006. Draft of 23rd February 2006.
12. Marta Kwiatkowska, Gethin Norman, and David Parker. PRISM: Probabilistic model checking for performance and reliability analysis. *ACM SIGMETRICS Performance Evaluation Review*, 36(4):40–45, 2009.
13. Marta Kwiatkowska, Gethin Norman, and Jeremy Sproston. Probabilistic model checking of the IEEE 802.11 wireless local area network protocol. In *Proceedings of the 2nd Joint International Workshop on Process Algebra and Probabilistic Methods and Performance Modeling in Verification (PAPM-PROBMIV 2002)*, volume 2399 of *Lecture Notes in Computer Science*, pages 169–187. Springer, 2002.
14. Marta Kwiatkowska, Gethin Norman, and Jeremy Sproston. Probabilistic model checking of deadline properties in the IEEE 1394 FireWire root contention protocol. *Formal Aspects of Computing*, 14(3):295–318, 2003.
15. Marie Duflot, Marta Kwiatkowska, Gethin Norman, and David Parker. A formal analysis of Bluetooth device discovery. International Journal on Software Tools for Technology Transfer (STTT), 8(6):621–632, 2006.
16. Marta Kwiatkowska, Gethin Norman, and David Parker. PRISM: Probabilistic model checking for performance and reliability analysis. *ACM SIGMETRICS Performance Evaluation Review*, 36(4):40–45, 2009.
17. Athanassis Boulis, Ansgar Fehnker, Matthias Fruth, and Annabelle McIver. Cavi: Simulation and model checking for wireless sensor networks. In *Proceedings of the 5th International Conference on the Quantitative Evaluation of Systems (QEST 2008)*, pages 37–38, 2008.
18. Karim Seada, Marco Zuniga, Ahmed Helmy, and Bhaskar Krishnamachari. Energy efficient forwarding strategies for geographic routing in lossy wireless sensor networks. In *Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems, SenSys 2004*, pages 108–121. ACM Press, 2004.
19. Bo Han a,*, Weijia Jia b, Lidong Lin (2007), Performance evaluation of scheduling in IEEE 802.16 based wireless mesh networks, Elsevier 30 (2007) 782–792
20. Cremers, C. J. (2008, January). The Scyther Tool: Verification, falsification, and analysis of security protocols. In *Computer Aided Verification* (pp. 414-418). Springer Berlin Heidelberg.
21. Xu, Sen, Chin-Tser Huang, and Manton M. Matthews. "Modeling and analysis of IEEE 802.16 PKM Protocols using CasperFDR." In *Wireless Communication Systems. 2008. ISWCS'08. IEEE International Symposium on*, pp. 653-657. IEEE, 2008.
22. Komu, Beth N., Mjumo Mzyece, and Karim Djouani. "Formal Verification of Hash-based Authentication Protocol in WiMAX Networks."
23. Ölveczky, Peter Csaba, and Stian Thorvaldsen. "Formal modeling, performance estimation, and model checking of wireless sensor network algorithms in Real-Time Maude." *Theoretical Computer Science* 410.2 (2009): 254-280.
24. Gawanmeh, Amjad. "Embedding and Verification of ZigBee Protocol Stack in Event-B." *Procedia Computer Science* 5 (2011): 736-741 Elsevier.
25. Clarke, Edmund M., and Jeannette M. Wing. "Formal methods: State of the art and future directions." *ACM Computing Surveys (CSUR)* 28.4 (1996): 626-643.
26. J. Abrial, Modelling in Event-B: System and Software Engineering, Cambbridge University Press, 2009.
27. J.-R. Abrial, A system development process with Event-B and the RODIN platform, in: Proceedings of International Conference on Formal Engineering Methods, ICFEM'07, in: Lecture Notes in Computer Science, vol. 4789, Springer-Verlag, 2007, pp. 1–3.
28. Rodin Platform. http://www.event-b.org, 2010.