FORMAL METHODS AND NETWORK SECURITY PROTOCOLS: A SURVEY

Shabir Ahmad[1], Bilal Ehsan[1], Mohib Ullah[2], Imran Anjum[3]
[1]Government College of Commerce, Multan
Email: mian_shabbir@hotmail.com (Corresponding Author)
[2]Department of Computer Science, NFC-Institute of Engineering and Technology, Multan
[3]Department of Information Technology, BZ University, Multan

ABSTRACT*- In critical systems, formal methods are used for specification and verification. Official methods describe the security characteristics performs verifying the incorrect protocol properties. Communication protocols, especially security protocols, are another area where work is extremely necessary features and image accuracy features. Many stylistic models were developed from the moment they appear. The purpose of this survey is to bridge the gap between security requirements and formal requirements for design. In this paper, a study of wireless and secure networks is available in a variety of formal models that focus on the context of mobile applications. In this study the main work is the survey that find outs different threats to wireless security protocols and the application of formal methods for automated analysis of emerging weakness is in necessary in the modern age in the field of research.*

KEYWORDS: Wireless Security Protocols, Formal Methods, Formal Models, Scyther, FDR, CSP, Spin, ZigBee, AVISPA.

1. INTRODUCTION

Formal methods and tools are based on mathematical logic. Software identification, as well as system hardware, formal methods are used for verification and validation [1, 3]. Formal methods, specification (written in natural language) is a way to get mathematical equivalent. Therefore, it is normally used in the phases of SDLC analysis and design. Natural language often vague, contains incomplete and inconsistent statements. For example, when a specification translates a mathematical form into English, it will remove all the ambiguities and uncertainties in these statements. The official method can also include all possible variables and functions that may be hidden behind the English language makes the whole perspective. This representation Z, VDM, etc. Algebra. As you can make use of a number of official languages. Official methods can also be useful for checking features specified in the model. This evidence will be automatically performed interactively with models using the controller or test vehicles. Official specification and security analysis, has a long history of research in the development of computing up network protocols. Privacy protocols, authentication and security features such incorrectness has been confirmed by official methods [4, 5]. Figure 1 shows the procedure of the formal approach.

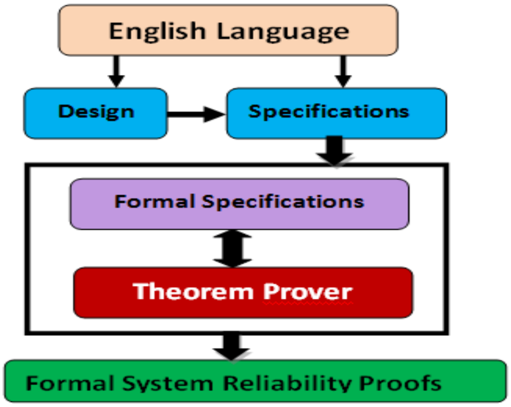


Figure 1: Formal Approach Procedure [2]

2. Formal Models for Security Protocols

In this paper, the specification of wireless network security protocols, describes the use of formal verification and validation methods. In the paragraphs that follow, specifying wireless security protocols, verifying and validating the method used for the current image, it appears a brief questionnaire containing details on modeling and security enhancements are available.

2.1 Formal Analysis of IKEv1 and IKEv2

ETH Zurich and Cas Cremers [6] IKEv1 and IKEv2 [7] in the analysis used the approach adopted by Meadows. Dolev and follow the Yao Un study line [8]. The authors focused on determining the logical weakness of encryption protocols and, unless they do not know the decryption key, assume that nothing is perfect, in the sense that learning a message encrypted with the enemy. This can be seen as the separation of concerns: research, based on the specifications used encryption algorithms. A second assumption is that the enemy has complete control over the network and can cut any message or change or add their own message. This analysis covers Ike A much more than the previous official analysis of security aspects. Bellara [9] discovered by key exchange according to the concepts of security, perfect direct confidentiality, key identity compromise impersonation and consider the various advanced security features such known key attacks. The research, are monitoring the basin, and the Cremers formality [10]. In addition, multiple protocol interactions between an example attack protocols also take into account [11,12,13]. Figure 2 shows the IKE secure system.

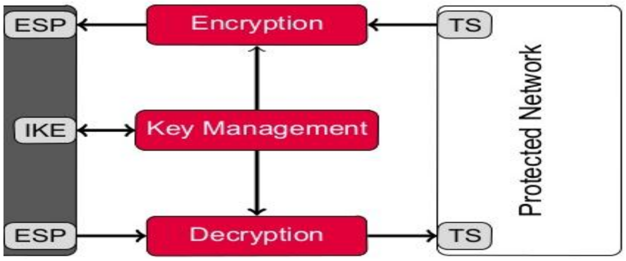
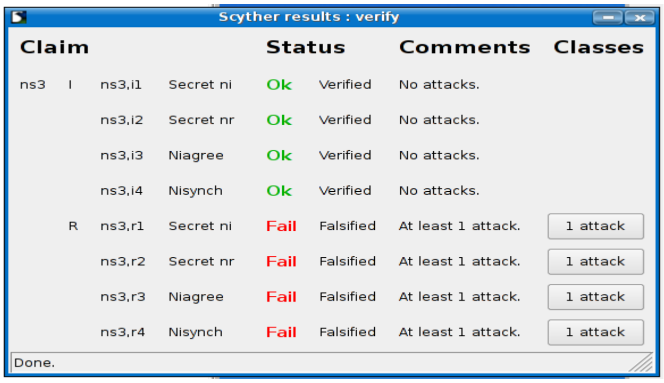


Figure 2: IKE Encryption [12]

2.2 A Formal Analysis using Scyther Tool

Scythe, verification, proven to be an effective tool is an automated tool for fraud analysis security protocol and security protocols. The protocols can be confirmed by ending the session with an unlimited number and guaranteed. The only available means capable of verifying synchronization [14]. Synchronization defines in the same way driven by the description of the protocol of the message. In other words, when a sensitive primer and completed the study protocol by protocol R and R I. completed. Then, all taken in the order described by the protocol messages that are sent. Scythe is, with the symbolic state again to look for technique to analyze the security protocols. Athena retrospective method based on the symbolic technique with the state of the search engine Aracne [14]. Engine of Arachne, lies the claim that the attack was broken by looking back. This technique allows full type defect and explore endless state field. Unlike Athena A Scythe, you can verify authentication functions such as synchronization as described and can handle several keys and non-atomic key structures. Scythe will also be used to verify different versions of PCC protocols [15]. The model analyzes the pkmv1 authentication protocol and the pkmv2'n vulnerability in both versions. In image analysis, key material theft is nowhere distributed with the privacy uniqueness and possible claims service is available in pkmv1 and pkmv2. However, both versions are broken down into PCC false identities and information privacy. It is expected that the revised IEEE 802.16 authentication protocol (e) provide a more secure platform. Figure 3 discloses a result of the trimmer verification tool.



Claim				Status		Comments	Classes
ns3	I	ns3,i1	Secret ni	Ok	Verified	No attacks.	
		ns3,i2	Secret nr	Ok	Verified	No attacks.	
		ns3,i3	Niagree	Ok	Verified	No attacks.	
		ns3,i4	Nisynch	Ok	Verified	No attacks.	
	R	ns3,r1	Secret ni	Fail	Falsified	At least 1 attack.	1 attack
		ns3,r2	Secret nr	Fail	Falsified	At least 1 attack.	1 attack
		ns3,r3	Niagree	Fail	Falsified	At least 1 attack.	1 attack
		ns3,r4	Nisynch	Fail	Falsified	At least 1 attack.	1 attack

Done.

Figure3: Scyther Verification [15]

2.3 Formal Verification of IEEE 802.11 using FDR/CSP

FDR (Failure Divergence Refinement) is a formal verification tool used for the formal verification based on a state machine. CSP first by Hoare [16, 17] are described and applied in many fields. FDR controls provide authentication and privacy features described by the CSP. The safety model does not meet these specifications [18], which is defined by the possible FDR connection. In recent years, a method for analyzing the security protocol has been established. Model using CSP, then confidentiality, authentication and other features were confirmed using FDR [19,20,21]. In this method, the most difficult task is to determine the behavior of the security protocol using CSP. Protocol security Gavin Lowe CSP to simplify expression, was casperfd [22] developed. Many communications protocol has been confirmed by casperfd. The random simulations performed on a protocol have the ability to produce as well as the CSP program. This program is used to make an effective verification of the correction of protocol specifications. However protocol, specification language protocol (SPL) must be modeled in a high-level language called. Casperfd, you can perform a thorough verification can be set with mathematical security. Figure 4 shows the fdr'n IDE.

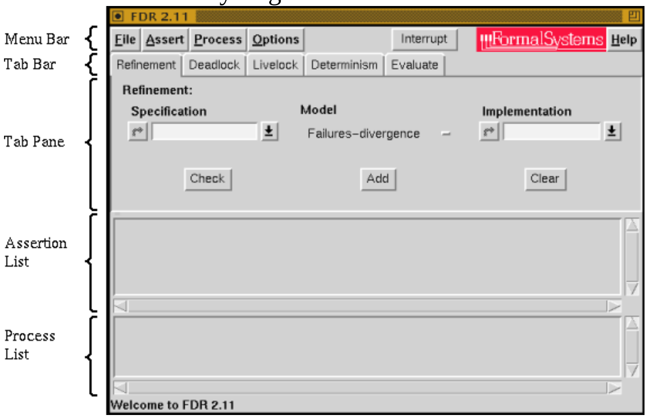


Figure 4: IDE of FDR [19]

2.4 Testing and Validation of Wireless Protocols by Spin Model Checker

A network configuration Bluetooth Solution (BLN) for different official testing and testing techniques and the tools used to analyze the protocol. This network, networking automatically when the system started was created using Bluetooth static nodes. After restructuring, BLN, m-commerce, location or networking context-aware such as museums or email provides location services for wireless environments. BLN configuration was initially defined in natural language and some initial testing and analysis based on the simulation of the past. Official methods have provided a deeper understanding of some failure scenarios and reveal unexpected errors. PROMEL and spinning companion [23] tool was selected to support the verification process. Giro is aimed at verifying the efficient and high-level PROMEL software to specify the system description (Meta processor language) language used. Spin tool, used to track errors in the logical design of distributed systems, such as data communication protocols. This tool checks the logical consistency of a specification and locks, missing flags, unspecified receptions, and processes requests information about race conditions. Spin, used to create a high level of on-the-fly validation program has been optimized specifications. This validated is compiled and executed. Accuracy is determined when the accusations against samples have been sent back in the interactive simulator, and we have examined in detail to identify and eliminate the cause, so the desired configuration has BLN propose an alternative version of the protocol. When creating a validator, the result of each centrifuge process template is translated into a vending machine. The concurrent behavior of the global system, an automated asynchronous process automated by the behavior - in our case one per node automatically in addition to automata and is obtained by calculating the processes used for modeling. The resulting global system behavior, however, is represented as an automatic. This product insertion, system state or graph of global accessibility [24] is called. Figure 5 shows the rotational model phases.

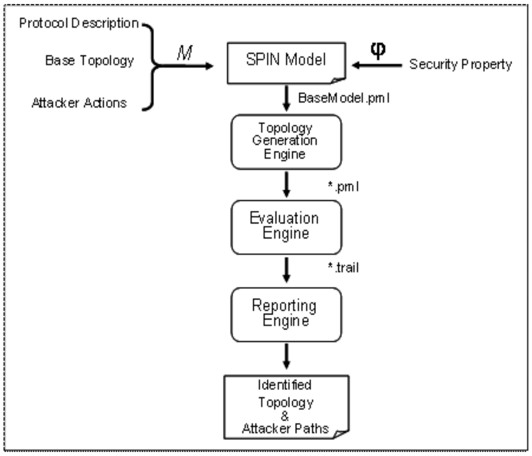


Figure 5: Process of SPIN Model [24]

2.5 Verification of ZigBee Protocol

ZigBee [25] The IEEE 802.15.4 standard is to add a specification to improve network and security layers. Wireless Sensor Networks (WSN) also includes an application framework for high-level communication. ZigBee is required for wsn'n operation; Verification of design accuracy is required. Official methods can efficiently be used to verify a wide range of systems, including the features of the ZigBee protocol stack [26, 27]. Case B formal verification method is used to allow the incorporation of event B modeling stack protocol protocol ZigBee primitive and verified [28]. This approach fits the protocol layer design characteristics of the different levels of abstraction will benefit from the ability to model the incident method B.

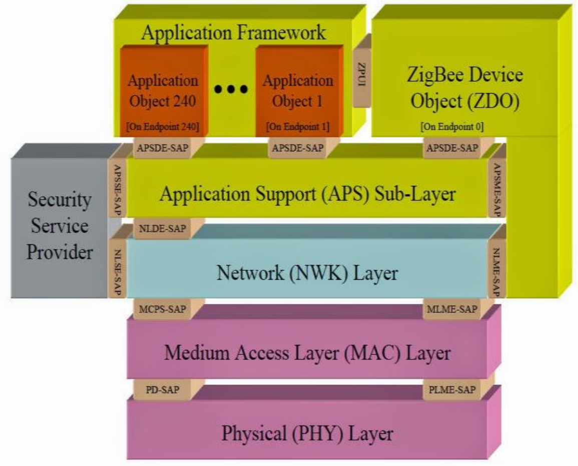


Figure 6: ZigBee Protocol Stack [28]

2.6 FDR Model Checking

PAP and the protocol model name authentication model EAP-MD5 refer to FDR as the control. This model focuses on the IEEE 802.1x protocols used as a basis to improve the security of wireless networks. Kim II-Gon and Choi Jin-Young. Casper and CSP model as an official PAP and EAP-MD5 [29, 30] in the security protocols and check the use of the FDR security functions. At the same time, attacks and security breaches are open to moderates and show that possible measures were discussed.

2.7 FADES and Security Properties

Hasan, Riham et al. Provide FADES (Formal Analysis and Design Approach for Engineering Security) integrated with KAOS (Information on Automatic Specification) and B specification language [31] to derive safety design specifications and to get more applications from security requirements. A case study demonstrates the ability of the spy network system to address changes in security requirements by introducing corrective changes in security requirements. The objective is to close the gap between design and security requirements for formal requirements..

2.8 AVISPA Model

AVISPA model, , which tinysec three complementary protocol as official, LEAP and tinypky is analyzing [32]. This model is used in HLPSL languages and is used as a Wasp control model tool. Wasp two main security features, checks the reliability and confidentiality of messages. Two attacks were detected during the analysis; One of them is privacy, and the other was a hidden attacker to access the data [33]. The AVISPA verification process is illustrated in Figure 7.

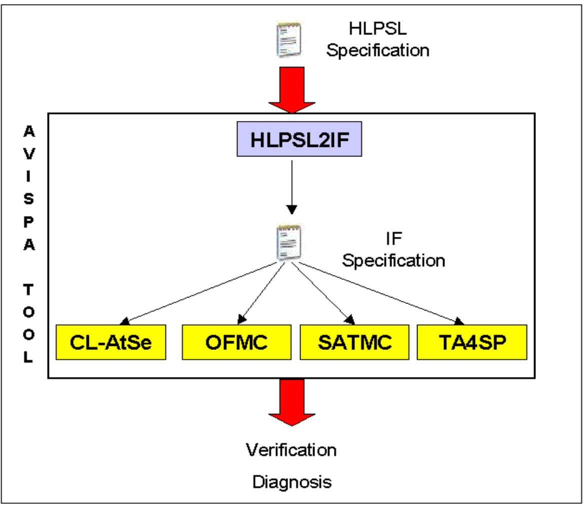


Figure 7: AVISPA Tool Process of Verification [32]

3. DISCUSSIONS

Currently, some formal methods have been developed that are effective method. Most of the model protocols described above are based on analysis and verification. They are just some automated tool support. These tools are only for analysis of security protocols and also have the ability to confirm synchronization. These media can also operate on non-atomic keys and multiple key structures. Describing the safety features of official cars and improper protocol specifications performs effectively being verified. Inconsistency and lack of such problems, there is no proper analysis of protocol specifications remain there.

The complete automation of the test process, to provide a required behavior model system protocol requires the use of formal methods. It will be proved suitable model for the correct problem modeled the importance of the characteristics, interests, ie control, the data have demonstrated one and the specification of different aspects of communication. Faster wireless services with no official model assistance for wireless network security protocols, lowering the cost of network users to more security advantages such as ensuring they use. Integration official model, interoperability, agile development provides benefits such as scalability and profitability.

Table 1: Comparison of Tools

Platform/Protocol	Tool	Formal Findings
IKEv1 & IKEv2	Cryptography	Analysis
PKM, PKMv2	Scyther	Analysis, Verification
IEEE 802.11	FDR, CSP	
BLN	Spin, Promela	Verification
ZigBee	Event-B	Verification
PAP, MD5	FDR	Verification
KOAS	FADES	Specification, Requirements
TinySec, LEAP, TinyPK	AVISPA	Verification

4. Conclusion

In this brief study, a series of official vehicles is presented. Scythe, verification, proven to be an effective tool is an automated tool for fraud analysis security protocol and security protocols. FDR and ensures authentication and security features such as CSP. Spin tool, used to track errors in the logical design of distributed systems, such as data communication protocols. ZigBee, IEEE 802.15.4 standard is a specification to add to improve networking and security layers. FDR model is mainly used to improve the safety of wireless networks. Wasp two main security feature, checks the reliability and confidentiality of messages. Various threats and weaknesses in the existing model of all wireless network protocols and model approach has limitations in rigorous analysis. First, there is a need for future research into threats and automatically analyze weaknesses. Second, on the application of formal methods to research needs emerged wireless security protocols. Threats can be formally described by a formally specified language and can be analyzed by a model checker.

REFERENCES

1. M. Bugliesi, R. Focardi, M. Maffei, Authenticity by tagging and typing, in: FMSE ’04: Proceedings of the 2004 ACM Workshop on Formal Methods in Security Engineering, ACM Press, New York, NY, USA, 2004, pp. 1–12.
2. Ahmad, Shabir, Shafiq Hussain, and Muhammad Farooq Iqbal. "A FORMAL MODEL PROPOSAL FOR WIRELESS NETWORK SECURITY PROTOCOLS." *Science International* 27.3 (2015).
3. M. Abadi, M. Burrows, R. Needham. “A Logic of Authentication”, Proceeding of the Royal Society, Series A, pp. 233-271, December 1989.
4. Kim, Il-Gon, and Jin-Young Choi. "Formal verification of PAP and EAP-MD5 Protocols in wireless networks: FDR Model Checking." *Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference on*. Vol. 2. IEEE, 2004.
5. P.Y.A. Ryan and S.A. Schneider, “Modeling and analysis of security protocols: the CSP Approach”, Addison-Wesley, 2001.
6. Cremers, Cas. Key exchange in IPsec revisited: formal analysis of IKEv1 and IKEv2. Springer Berlin Heidelberg, 2011.
7. Basin, David, Cas Cremers, and Catherine Meadows. "Model checking security protocols." *Handbook of Model Checking* (2011).
8. Dolev, Danny, and Andrew C. Yao. "On the security of public key protocols." *Information Theory, IEEE Transactions on* 29.2 (1983): 198-208.
9. Bellare, Mihir, Ran Canetti, and Hugo Krawczyk. "A modular approach to the design and analysis of authentication and key exchange protocols." In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pp. 419-428. ACM, 1998.
10. Basin, D., Cremers, C.J.F.: Modeling and Analyzing Security in the Presence of Compromising Adversaries. In: Computer Security - ESORICS 2010. Lecture Notes in Computer Science, vol. 6345, pp. 340{356. Springer (2010)
11. Cremers, Cas. "Feasibility of multi-protocol attacks." Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on. IEEE, 2006.
12. Kelsey, J., Schneier, B., Wagner, D.: Protocol interactions and the chosen protocol attack. In: Proc. 5th International Workshop on Security Protocols. Lecture Notes in Computer Science, vol. 1361, pp. 91{104. Springer-Verlag (1997)
13. M. Anlauff, D. Pavlovic, R. Waldinger, S. Westfold, Proving authentication properties in the Protocol Derivation Assistant, in: Pierpaolo Degano, Ralph Küsters, Luca Vigano (Eds.), Proceedings of FCS-ARSPA 2006, ACM, 2006.
14. Noudjoud, Kahya, Debbah Adel, and Nacira Ghoualmi. "WiMAX Security–A Formal Analysis using Scyther tool."
15. Scyther-C.J.F. Cremers, Scyther: automatic verification of security protocols. Available from: <http://www.win.tue.nl/ccremers/scyther/>.
16. C.A.R. Hoare, “Communicating sequential processes”, Communications of ACM, vol. 21, no. 8, pp.666–677, 1978.
17. C.A.R. Hoare, “Communicating Sequential Processes”, Prentice Hall International, 1985.
18. A.W. Roscoe, Modelling and verifying key-exchange protocols using CSP and FDR, Proceedings of the 8th IEEE Computer Security Foundations Workshop (CSFW 1995), IEEE Computer Society Press, Washington, 1995, pp. 98–107.
19. Lowe, Gavin. "Breaking and fixing the Needham-Schroeder public-key protocol using FDR." *Tools and Algorithms for the Construction and Analysis of Systems*. Springer Berlin Heidelberg, 1996. 147-166.
20. P.Y.A. Ryan and S.A. Schneider, “Modeling and analysis of security protocols: the CSP Approach”, Addison-Wesley, 2001.
21. S. Schneider, Verifying authentication protocols in CSP, IEEE Trans. Softw. Eng. 24 (9) (1998) 741–758, doi:10.1109/32.713329.

22. Lowe, Gavin. "Casper: A compiler for the analysis of security protocols." *Journal of computer security* 6.1 (1998): 53-84.
23. Holzmann, G., 2003. The SPIN Model Checker: Primer and Reference Manual. Pearson Education, Englewood Cliffs, NJ.
24. Ahmad, Shabir, and Bilal Ehsan. "The Cloud Computing Security Secure User Authentication Technique (Multi Level Authentication)." *IJSER* 4.12 (2013): 2166-2171.
25. Gawanmeh, Amjad. "Embedding and Verification of ZigBee Protocol Stack in Event-B." *Procedia Computer Science* 5 (2011): 736-741.
26. L. Chunqing and Z. Jiancheng. Research of ZigBee's Data Security and Protection. In IEEE International Forum on Computer Science-Technology and Applications, pages 298–302. IEEE Computer Society Press, December 2009.
27. ZigBee Alliance. WPAN Industry Group, http://www.zigbee.org, 2010.
28. J. Abrial, Modelling in Event-B: System and Software Engineering, Cambridge University Press, 2009.
29. Kim, II-Gon, and Jin-Young Choi. "Formal verification of PAP and EAP-MD5 Protocols in wireless networks: FDR Model Checking." *Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference on*. Vol. 2. IEEE, 2004.
30. G. Lowe, Breaking and fixing the Needham-Schroeder public-key protocol using FDR, in: Proceedings of TACAS, Lecture Notes in Computer Science, vol. 1055, Springer, 1996, pp. 147–166.
31. Hassan, Riham, et al. "Integrating formal analysis and design to preserve security properties." *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*. IEEE, 2009.
32. Tobarra, Llanos, et al. "Model checking wireless sensor network security protocols: Tinysec+ LEAP." *Wireless Sensor and Actor Networks*. Springer US, 2007. 95-106.
33. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, L. Vigneron, The AVISPA tool for the automated validation of internet security protocols and applications, in: Proceedings of Computer Aided Verification'05 (CAV), Lecture Notes in Computer Science, vol. 3576, Springer, 2005, pp. 281–28