I.J. Information Technology and Computer Science, **2019, 12, 30-37**
Published Online December 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2019.12.03

A Comparative Analysis of Tools for Testing the Security Protocols

Reham Abdellatif Abouhogail
Electrical Quantities Metrology Dept. National Institute of standards (NIS), Egypt
E-mail: rehlatif@yahoo.com

Received: 09 October 2019; Accepted: 25 October 2019; Published: 08 December 2019

***Abstract*—**In this paper, Analysis and comparison of two popular security verification tools namely Automated Validation of Internet Security Protocols and Applications (AVISPA) and Burrows-Abadi-Needham (BAN) logic are presented in terms of the usability, complexity, and other properties of the selected tools. The comparison shows the benefits and the drawbacks for the two tools. As a case study, two previously proposed security protocols, which were tested before by BAN logic only are evaluated and proved using the automated verification tool AVISPA to ensure that these protocols satisfy the other main security measures.

***Index Terms*—**AVISPA, Authentication protocols, BAN Logic, Handover, Privacy, Wimax.

I. Introduction

Security protocols are mathematical procedures, that require tools that use methods of mathematics and logic to carry out analysis [1]. Analysis and verification of the proposed security protocols are considered very important steps towards applying these protocols safely. Moreover, sometimes verification of the protocols detects unnecessary steps when eliminated this reduces the cost and the computation overhead of the implementation of these protocols.

In the current paper, we have chosen two popular verification tools, which are related to two verification methodologies. They are the Automated Validation of Internet Security Protocols and Applications (AVISPA) toolkit [2], which is related to automated approach, and the Burrows-Abadi-Needham (BAN) logic tool [3], which is related to belief logic. Most of the recent researches that use a verification tool to test their new proposed protocols use one of these two tools under discussion [4, 5, 6, 7, 8]. Others use both of them [9, 10]. Therefore, in this paper, we select these two verification tools and give a short and useful comparison which helps to differentiate between them. Moreover, this comparison is considered as a direction to retest two previously proposed security protocols that were tested before by the logical verification tool, which is called BAN logic.

We select two previously proposed protocols. They are [11], and [12]. The causes for choosing these protocols are: first, the mutual authentication between the user and the access point is required in both of them. Second, these proposed protocols were previously tested using BAN logic only. Third, replay and Man in the Middle attack are considered one of the most important attacks that can cause problems in these protocols. So the previous three reasons make these tools appropriate for our comparison. After testing them using AVISPA, we expect to be either more confident from the immunity of these protocols against some types of attacks much more than before or we will show new weak points which were not known before.

The Contributions in this paper

- The paper presents a new comparison in its kind, which compares AVISPA the most famous graphical automated tool, and BAN logic the most famous, easy logic and non-automated tool.
- To get the benefits of the AVISPA tool, simulation and verification of two previously proposed protocols using the AVISPA tool are presented in the current paper. They were verified previously using BAN logic. This step adds to these protocols which increases the trust in these two protocols and considered as a case study for the topic under discussion.

The rest of the paper is as follows, Section 2 describes the two selected verification tools and gives a qualitative comparison for the two selected tools. Section 3 gives a security analysis using the AVISPA tool for two previously proposed authentication protocols. In Section 4 we present the conclusion.

II. Description for the Two Selected Verification Tools

As mentioned before, one can find a series of tools for the verification of cryptographic protocols. We have selected AVISPA and BAN logic amongst all these for our comparative analysis. This decision is largely driven by the popularity of these two tools amongst all, we surveyed. The two mentioned tools are suitable for testing authentication protocols. P. Lafourcade and M. Puys made research in [13], that research made a comparison between different versions for twelve tools from the main automated tools. They focused on their comparison on the execution time and the memory consumption for these automated tools that can deal with the Exclusive-Or (XOR) and the Diffie-Hellman (DH) characteristics, as OFMC [14], CL-Atse [15], Scyther [16], Tamarin [17], TA4SP [18], and extensions of ProVerif [19, 20]. They concluded in their paper that there isn't a clear winner in this competition. So each tool has its own advantages and its own disadvantages. Therefore, in the current paper, we chose one of these main automated tools, that tool is AVISPA because it has four different back-ends to make our comparison with one of the non-automated tools, the BAN logic. In this section, we depict the vital characteristics of these two tools.

A. AVISPA

AVISPA is a push-button tool for the automated validation of internet security-sensitive protocols and applications [2]. It presents a modular and expressive formal language for specifying protocols and their security characteristics and supports four back-ends that provide a variety of methods for automatic analysis techniques [2]. The four back-ends are The On-the-Fly Model-Checker (OFMC), the Constraint-Logic-based Attack Searcher (CL-AtSe), the SAT-based Model-Checker (SATMC), and the TA4SP protocol analyzer [21]. They verify protocols by implementing tree automata-based on automatic approximations [21]. All the back-ends of the tool analyze protocols under the assumptions of perfect cryptography and that the protocol messages are exchanged over a network that is under the control of a Dolev-Yao intruder [21].

A user talks to the tool by expressing the required security protocol in the High-Level Protocol Specification Language (HLPSL). The HLPSL is a modular expressive, role-based, formal language that permits for the specification of control-flow patterns, data constructions, different cryptographic operators and their algebraic characteristics, different adversary models, as well as complex security properties [21]. These features give the user the ability to model protocols in HLPSL directly without simplifying the protocols first, as is done in other approaches [21]. Using the HLPSL translator the AVISPA tool automatically converts a user's security protocol into the equivalent specification written in the Intermediate Format (IF). Then the IF specifications inserted to the back-ends of the AVISPA Tool. The back-ends implement different techniques to search for possible attacks according to the presented properties of the protocols [21]. In the end, the AVISPA tool provides the user with the results of its analysis. The results are common between the four back ends and exactly defined. Output format declaring whether the requirements were satisfied. If an attack is found in the protocol under test, the tool displays it as a message-sequence chart. Because of the difficulty of written the protocol under test in HLPSL language, it can be written in CAS+ language [22] which is more simple than HLPSL, then using the AVISPA translator to translate it to the HLPSL language [23]. Moreover, It’s widely believed to simulate internet protocols and makes the required security analysis [24].

B. BAN logic

Burrows, Abadi, and Needham developed BAN logic in 1989 [3]. BAN logic is considered a significant tool in the field of security protocol testing and analysis. It contains a number of rules. As the message meaning rule, the interpretation rule, the nonce verification rule, the jurisdiction rule, the freshness rule, and the synthetic rule, the work of BAN logic depends on:

- The beliefs of honest parties participated in the protocols, and
- The effect of these beliefs with the sequence of communication.

It depends on the logic of belief and action. Therefore, it cannot be used to prove a protocol flawed. Because there are no logical inversions. When the protocol flawed, the proof of its correctness can't be reached using BAN logic. As a result, some development for the BAN logic was proposed, Like GNY logic [25] and SVO logic [26]. These new enhancements solve some problems of BAN but they lack its simplicity. Table 1 shows a summary of the comparison between BAN and AVISPA.

Table 1. Comparison between BAN logic and AVISPA [1, 3].

Comparative point	BAN logic	AVISPA tool
1.The method of work.	Non- automatic tool.	An automatic tool.
2. Complexity.	Easy to use.	Rather difficult to use.
3. Prerequisites to use this tool.	1. Basics of security protocols. 2. Method and rules of BAN logic test.	1. Deep knowledge of the analyzed protocols. 2. Learn a new programming language (HLPSL).
4.Reliability.	Find some flaws.	Validate or detect flaws.
5. Usability	It cannot be used to prove a protocol flawed.	It can be used to prove a protocol flawed.
6.Method of analysis.	Analysis of each message of the protocol separately.	Analysis of all the messages that construct the protocol at the same time.
7. The tool has an efficiency in.	Ensures the security of the session keys among shared entities.	Check that the protocol under test is robust against replay and man-in-the-middle attacks

C. Qualitative Comparison

From the previous two subsections, we can say that the two presented methods of verification can verify the protocol. However, each method has some benefits than the other one. Therefore, we have reached to a comparison between BAN and AVISPA contains the main points as declared in Table 1. Nowadays, the direction of researchers for security testing is towards software automated tools although automated tools like any software programs may have some bugs. Because these tools are subjected to upgrading continuously when new vulnerabilities are discovered.

Although the difficulty when using AVISPA, the leading features for it than BAN lead us to reprove the previously proposed protocols but this time using the AVISPA automated tool. Especially, after Ban Logic couldn't identify the flaw in the known public - key protocol Needham-Shroeder as stated in [27], and NSPK and Ottway-Rees protocols as stated in [28]. In the next section, we present an application of verification using the most reliable tool, which is the AVISPA tool. Two previously proposed protocols [11, 12] will be described, then a security analysis for them will be presented using the AVISPA tool.

III. Security analysis using AVISPA for two Security protocols as a Case Study

In this section, we select two previously proposed protocols, that were tested using BAN logic to test them again, but this time using the AVISPA tool to get its benefits. In the beginning, we will give a brief description of the two protocols, which were proposed in [11, 12], then we will give analysis for them using the AVISPA automated tool. The used notations and acronyms will be found in Table.2.

Table 2. Notations

Notation & acronym	Description
MU	the Mesh STA User
HMP	Home Mesh Access Points
P_0	Initial pseudo random number
P_n	P_n=f(P_{n-1}); f: is a pseudo random function.
I_{MU}	ID number of MU
I_{MP1}	ID number of HMP1
T_{MU}	The credential ticket of the MU
K_{GB}	The group mesh access points key
$THMK_0$	A temporary handover mobile key
τ_{exp}	Expiration date and time of this ticket.
H	the first byte of the credential ticket
E_x(y)	Symmetric encryption of *y* by key *x*.
N^i_{MU}	A random number generated by *MU*
N^i_{MP}	A random number generated by *MP*
R_{MU}	A random number generated by *AS*
CMAC	Cipher-based Message Authentication Code
MAC	Message Authentication Code

A. Description of the two selected protocols

Fast Handover with Privacy Preserving Authentication Protocol for Mobile WiMAX Networks

Fast Handover with Privacy-Preserving Authentication Protocol for Mobile WiMAX Networks, which was proposed in [12] is a mutual authentication protocol as shown in Fig.1. It is a handover authentication scheme based on a ticket for the IEEE 802.16m network. In this scheme, the Mesh STA User (*MU*) and the Mesh Access Points (*MPs*) can complete the mutual authentication without the need to communicate with the AS server, thus the handoff delay is improved than before. This protocol uses symmetric encryption. The identity of *MU* is sent encrypted to preserve good privacy. Moreover, the ticket is changed for every hop to preserve good secrecy.

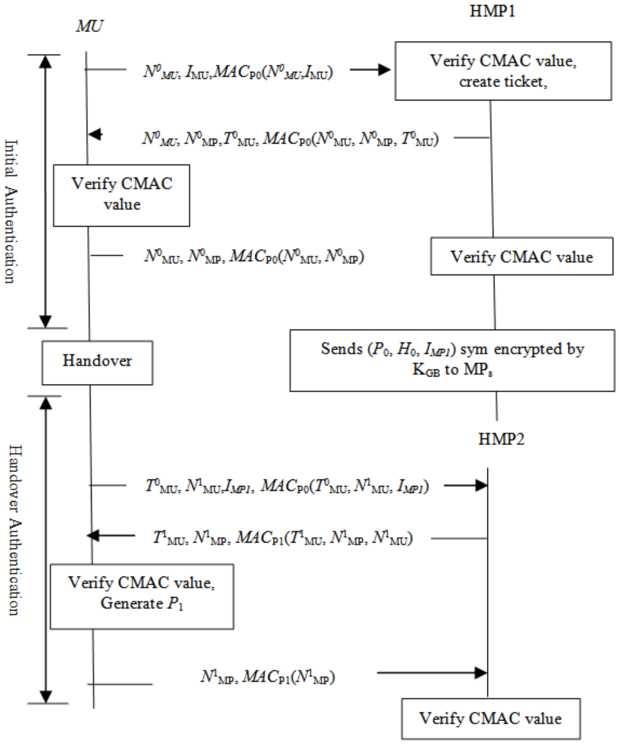

HMP1
MU
$N^0_{MU}, I_{MU}, MAC_{P0}(N^0_{MU}, I_{MU})$
Verify CMAC value, create ticket,
$N^0_{MU}, N^0_{MP}, T^0_{MU}, MAC_{P0}(N^0_{MU}, N^0_{MP}, T^0_{MU})$
Initial Authentication
Verify CMAC value
$N^0_{MU}, N^0_{MP}, MAC_{P0}(N^0_{MU}, N^0_{MP})$
Verify CMAC value
Handover
Sends (P_0, H_0, I_{MP1}) sym encrypted by K_{GB} to MP_s
HMP2
Handover Authentication
$T^0_{MU}, N^1_{MU}, I_{MP1}, MAC_{P0}(T^0_{MU}, N^1_{MU}, I_{MP1})$
$T^1_{MU}, N^1_{MP}, MAC_{P1}(T^1_{MU}, N^1_{MP}, N^1_{MU})$
Verify CMAC value, Generate P_1
$N^1_{MP}, MAC_{P1}(N^1_{MP})$
Verify CMAC value

Fig.1. Fast Handover with Privacy Preserving Authentication Protocol for Mobile WiMAX Networks [12].

Improving the Handoff Latency of the Wireless Mesh Networks Standard protocol

This protocol is an improvement to the IEEE 802.11-based wireless mesh networks in terms of the authentication delay. The main objective of the wireless mesh network is to facilitate and secure moving through the network. The proposed model is constructed of two phases as shown in Fig.2. They are the initial authentication phase and the handover authentication phase. The idea of this protocol is based on the redistribution of a key by the Mesh Home Access Points (*HMP*) to its neighbors. This proposed protocol guarantees a good definition to the *MU* when enters a new *MP*'s region. This is done without sending the *MU*'s identity. The strong level of privacy is considered one of the main features of this protocol.

B. Verification of the two selected protocols using AVISPA

We have implemented the two protocols in the HLPSL language. In our implementation, there are two basic roles, namely *ms* and *hps*, which represent the participants as the user and the Home Mesh Access Points, respectively as shown in Fig. 3 and Fig. 4 for the proposed protocol in [12] and Fig. 7 and Fig. 8 for the proposed protocol in [11]. In addition to giving the specifications for the composition rules in HLPSL as shown in Fig. 5 and Fig. 6 for the proposed protocol in [12], and Fig. 9 and Fig. 10 for the proposed protocol in [11]. They are the session and the environment rules. The environment rule is the top-level rule which defines the global constants and the composition of sessions, in which the intruder can take part in some roles as a legitimate user. All this depends on the specification of HLPSL. We have executed the test using CL-AtSe, OFMC, and SATMC back-ends. Using the Dolev- Yao model check, the back-ends check if there is any man-in-the-middle attack that may be executed by the intruder. The simulation results show that the two protocols are safe as shown in Figures 11, 12, 13, and 14. Therefore, we can say that they are free from passive and active attacks like the replay and man- in- the- middle attacks.

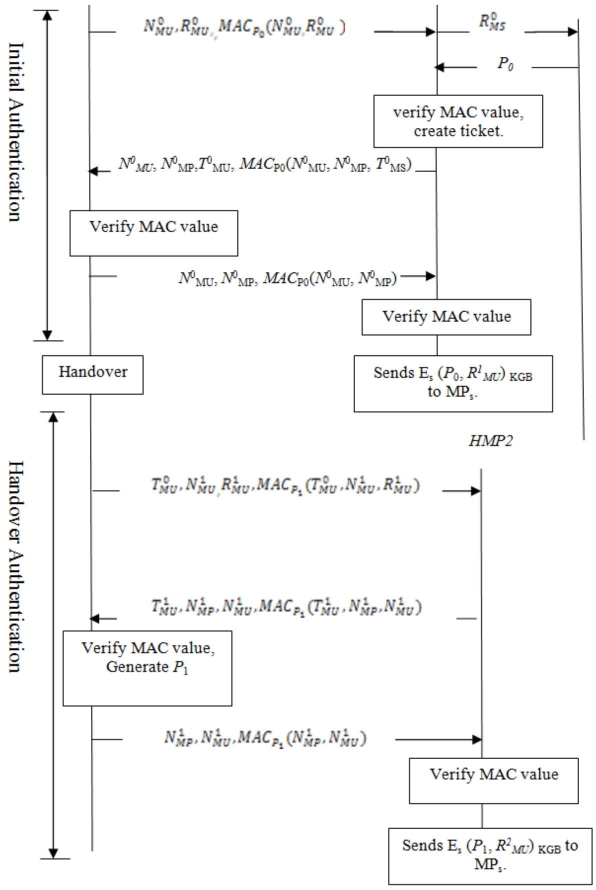
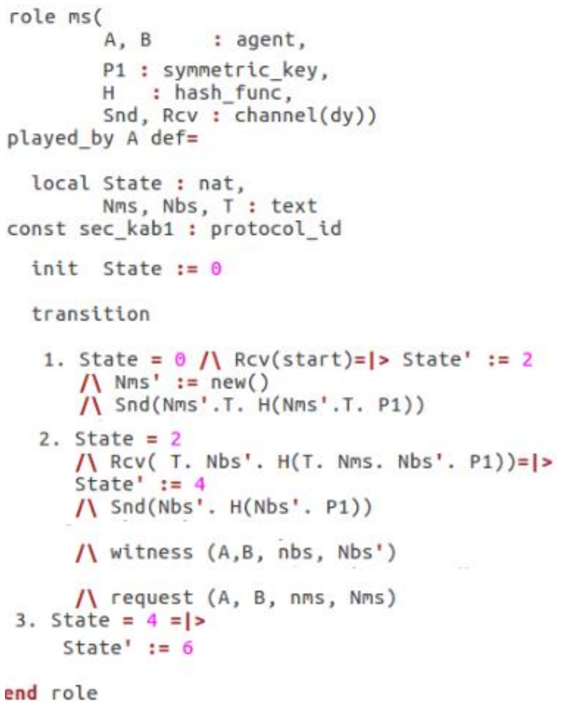
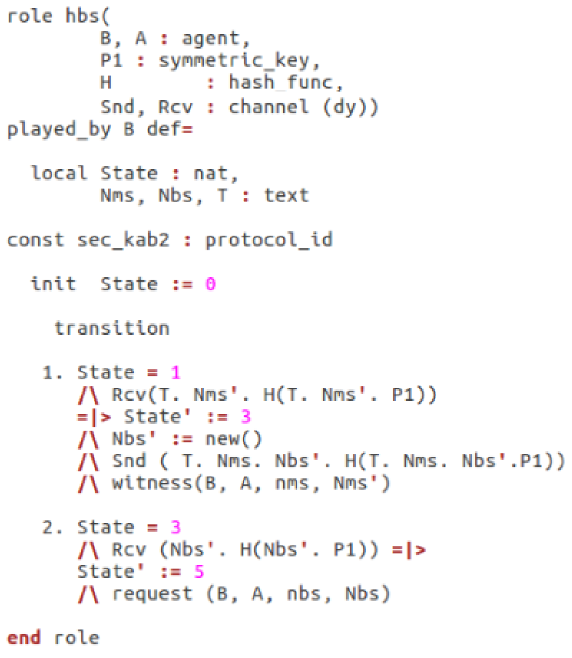

Initial Authentication
$N^0_{MU}, R^0_{MU}, MAC_{P_0}(N^0_{MU}, R^0_{MU})$
R^0_{MS}
P_0
verify MAC value, create ticket.
$N^0_{MU}, N^0_{MP}, T^0_{MU}, MAC_{P0}(N^0_{MU}, N^0_{MP}, T^0_{MS})$
Verify MAC value
$N^0_{MU}, N^0_{MP}, MAC_{P0}(N^0_{MU}, N^0_{MP})$
Verify MAC value
Handover
Sends $E_s(P_0, R^1_{MU})_{KGB}$ to MP_s.
HMP2
Handover Authentication
$T^0_{MU}, N^1_{MU}, R^1_{MU}, MAC_{P_1}(T^0_{MU}, N^1_{MU}, R^1_{MU})$
$T^1_{MU}, N^1_{MP}, N^1_{MU}, MAC_{P_1}(T^1_{MU}, N^1_{MP}, N^1_{MU})$
Verify MAC value, Generate P_1
$N^1_{MP}, N^1_{MU}, MAC_{P_1}(N^1_{MP}, N^1_{MU})$
Verify MAC value
Sends $E_s(P_1, R^2_{MU})_{KGB}$ to MP_s.

Fig.2. Improving the Handoff Latency of the Wireless Mesh Networks Standard Protocol [11].



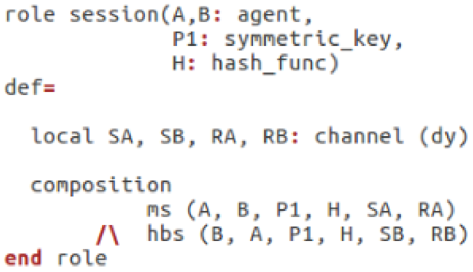
```
role ms(
        A, B      : agent,
        P1 : symmetric_key,
        H   : hash_func,
        Snd, Rcv : channel(dy))
played_by A def=

  local State : nat,
        Nms, Nbs, T : text
const sec_kab1 : protocol_id

  init  State := 0

  transition

   1. State = 0 /\ Rcv(start)=|> State' := 2
      /\ Nms' := new()
      /\ Snd(Nms'.T. H(Nms'.T. P1))

  2. State = 2
     /\ Rcv( T. Nbs'. H(T. Nms. Nbs'. P1))=|>
     State' := 4
     /\ Snd(Nbs'. H(Nbs'. P1))

     /\ witness (A,B, nbs, Nbs')

     /\ request (A, B, nms, Nms)
 3. State = 4 =|>
    State' := 6

end role
```

Fig.3. Role specification for the user of the proposed protocol in [12].



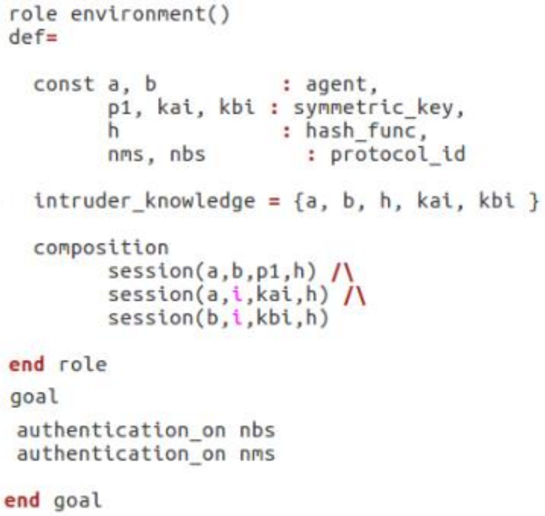
```
role hbs(
        B, A : agent,
        P1 : symmetric_key,
        H          : hash_func,
        Snd, Rcv : channel (dy))
played_by B def=

  local State : nat,
        Nms, Nbs, T : text

const sec_kab2 : protocol_id

  init  State := 0

    transition

   1. State = 1
      /\ Rcv(T. Nms'. H(T. Nms'. P1))
      =|> State' := 3
      /\ Nbs' := new()
      /\ Snd ( T. Nms. Nbs'. H(T. Nms. Nbs'.P1))
      /\ witness(B, A, nms, Nms')

   2. State = 3
      /\ Rcv (Nbs'. H(Nbs'. P1)) =|>
      State' := 5
      /\ request (B, A, nbs, Nbs)

end role
```

Fig.4. Role specification for the home mesh access points of the proposed protocol in [12]..



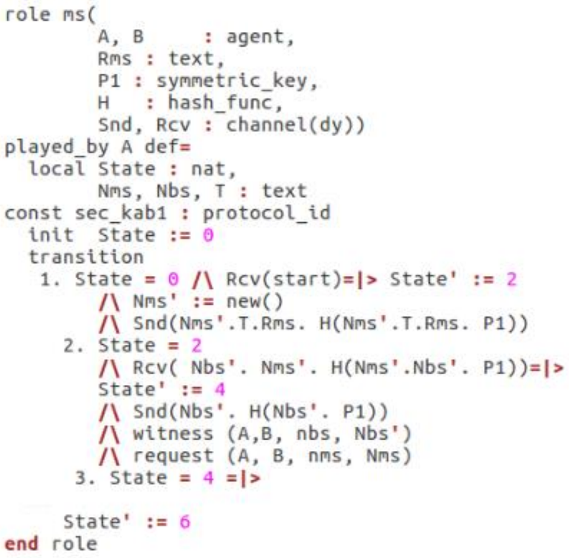
```
role session(A,B: agent,
             P1: symmetric_key,
             H: hash_func)
def=

  local SA, SB, RA, RB: channel (dy)

  composition
           ms (A, B, P1, H, SA, RA)
       /\  hbs (B, A, P1, H, SB, RB)
end role
```

Fig.5. Role specification for the session of the protocol proposed in [12]



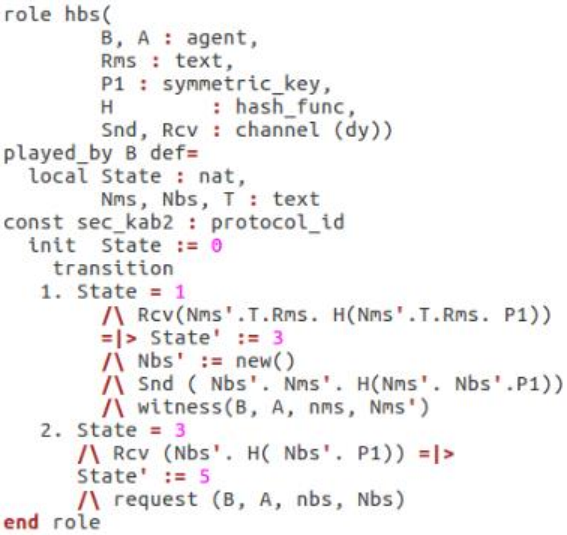
```
role environment()
def=

  const a, b           : agent,
        p1, kai, kbi : symmetric_key,
        h              : hash_func,
        nms, nbs        : protocol_id

  intruder_knowledge = {a, b, h, kai, kbi }

  composition
        session(a,b,p1,h) /\
        session(a,i,kai,h) /\
        session(b,i,kbi,h)

end role
goal
 authentication_on nbs
 authentication_on nms

end goal
```

Fig.6. Role specification for the goal and environment of the proposed protocol in [12].



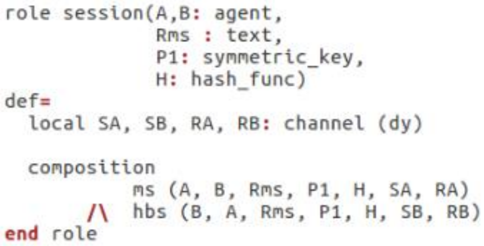
```
role ms(
        A, B      : agent,
        Rms : text,
        P1 : symmetric_key,
        H   : hash_func,
        Snd, Rcv : channel(dy))
played_by A def=
  local State : nat,
        Nms, Nbs, T : text
const sec_kab1 : protocol_id
  init  State := 0
  transition
   1. State = 0 /\ Rcv(start)=|> State' := 2
        /\ Nms' := new()
        /\ Snd(Nms'.T.Rms. H(Nms'.T.Rms. P1))
     2. State = 2
        /\ Rcv( Nbs'. Nms'. H(Nms'.Nbs'. P1))=|>
        State' := 4
        /\ Snd(Nbs'. H(Nbs'. P1))
        /\ witness (A,B, nbs, Nbs')
        /\ request (A, B, nms, Nms)
      3. State = 4 =|>

     State' := 6
end role
```

Fig.7. Role specification for the user of the proposed protocol in [11].



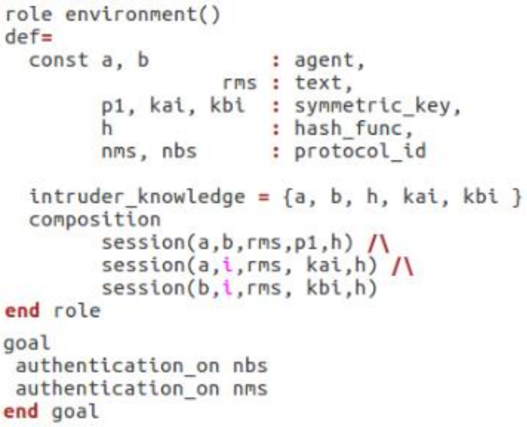
```
role hbs(
        B, A : agent,
        Rms : text,
        P1 : symmetric_key,
        H          : hash_func,
        Snd, Rcv : channel (dy))
played_by B def=
  local State : nat,
        Nms, Nbs, T : text
const sec_kab2 : protocol_id
  init  State := 0
    transition
   1. State = 1
        /\ Rcv(Nms'.T.Rms. H(Nms'.T.Rms. P1))
        =|> State' := 3
        /\ Nbs' := new()
        /\ Snd ( Nbs'. Nms'. H(Nms'. Nbs'.P1))
        /\ witness(B, A, nms, Nms')
   2. State = 3
      /\ Rcv (Nbs'. H( Nbs'. P1)) =|>
      State' := 5
      /\ request (B, A, nbs, Nbs)
end role
```

Fig.8. Role specification for the home mesh access points of the proposed protocol in. [11].



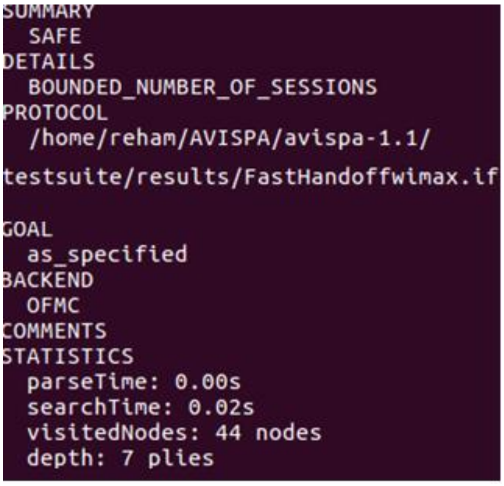
```
role session(A,B: agent,
             Rms : text,
             P1: symmetric_key,
             H: hash_func)
def=
  local SA, SB, RA, RB: channel (dy)

  composition
          ms (A, B, Rms, P1, H, SA, RA)
      /\  hbs (B, A, Rms, P1, H, SB, RB)
end role
```

Fig.9. Role specification for the session of the protocol proposed in [11].



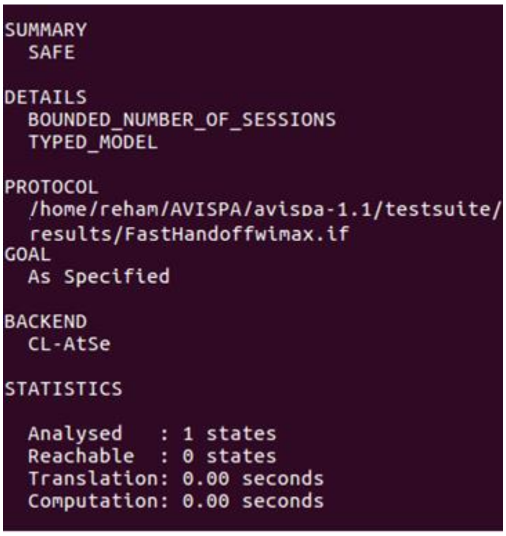
```
role environment()
def=
  const a, b           : agent,
                   rms : text,
        p1, kai, kbi  : symmetric_key,
        h              : hash_func,
        nms, nbs       : protocol_id

  intruder_knowledge = {a, b, h, kai, kbi }
  composition
        session(a,b,rms,p1,h) /\
        session(a,i,rms, kai,h) /\
        session(b,i,rms, kbi,h)
end role

goal
 authentication_on nbs
 authentication_on nms
end goal
```

Fig.10. Role specification for the goal and environment of the proposed protocol in [11].



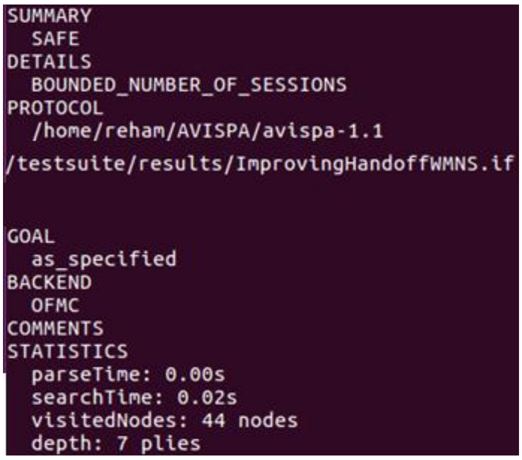
```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/reham/AVISPA/avispa-1.1/
testsuite/results/FastHandoffwimax.if

GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.02s
  visitedNodes: 44 nodes
  depth: 7 plies
```

Fig.11. The results of the analysis using OFMC of Fast Handover with Privacy Preserving Authentication Protocol for Mobile WiMAX Networks.



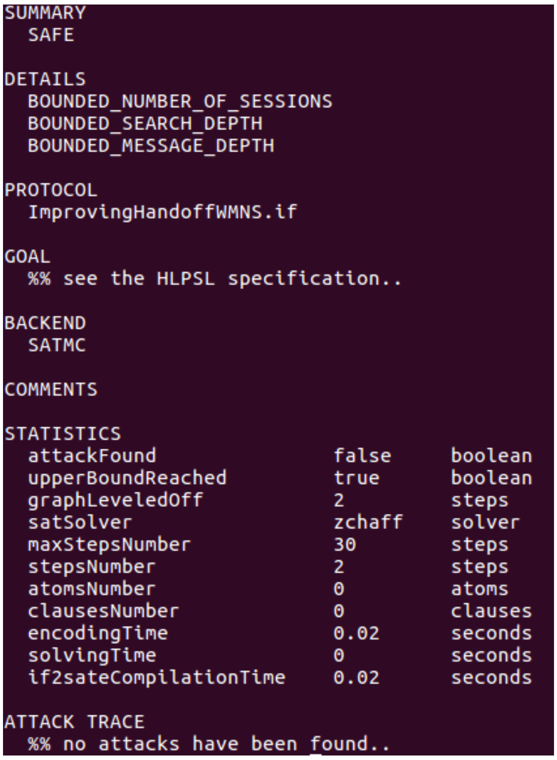
```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/reham/AVISPA/avispa-1.1/testsuite/
  results/FastHandoffwimax.if
GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 1 states
  Reachable  : 0 states
  Translation: 0.00 seconds
  Computation: 0.00 seconds
```

Fig.12. The results of the analysis using CL-AtSe of Fast Handover with Privacy-Preserving Authentication Protocol for Mobile WiMAX Networks.



```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/reham/AVISPA/avispa-1.1
/testsuite/results/ImprovingHandoffWMNS.if


GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.02s
  visitedNodes: 44 nodes
  depth: 7 plies
```

Fig.13. The results of the analysis using OFMC of Improving the Handoff Latency of the Wireless Mesh Networks Standard protocol.



```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  BOUNDED_SEARCH_DEPTH
  BOUNDED_MESSAGE_DEPTH

PROTOCOL
  ImprovingHandoffWMNS.if

GOAL
  %% see the HLPSL specification..

BACKEND
  SATMC

COMMENTS

STATISTICS
  attackFound              false     boolean
  upperBoundReached        true      boolean
  graphLeveledOff          2         steps
  satSolver                zchaff    solver
  maxStepsNumber           30        steps
  stepsNumber              2         steps
  atomsNumber              0         atoms
  clausesNumber            0         clauses
  encodingTime             0.02      seconds
  solvingTime              0         seconds
  if2sateCompilationTime   0.02      seconds

ATTACK TRACE
  %% no attacks have been found..
```

Fig.14. The results of the analysis using SATMC of Improving the Handoff Latency of the Wireless Mesh Networks Standard protocol.

IV. Conclusion

In this paper, we selected the BAN logic tool, and the AVISPA automated tool and present a comparison between them. The comparison declares that both of the two tools have useful characteristics. There seem to be some security benefits when choosing AVISPA. But AVISPA has some difficulty in use and needs more prerequisites than the needed prerequisites that the user needs when he starts to use BAN. Moreover, this paper is considered as an extension for two previously proposed protocols. These protocols are: 1- Fast Handover with Privacy Preserving Authentication Protocol for Mobile WiMAX Networks. 2- Improving the Handoff Latency of the Wireless Mesh Networks Standard Protocol. Where, after the results of the mentioned comparison, we see that we have to retest these previously proposed protocols again but this time using the AVISPA automated tool. The test proves that the two previously proposed protocols are safe and free from the replay and man- in-the- middle attacks. Our future work is to extend the comparison to include more security verification tools. Then using these tools to test number of previously proposed security protocols to show if they have any weak points.

ACKNOWLEDGMENT

This work was supported by the National Institute of Standards (NIS), Egypt. Also, I thank Eng. Muhammad H. G. ElSheikh for his help to solve the problems, that I faced when using the Ubuntu operating system.

REFERENCES

[1] Sebastian Mödersheim and Luca Vigano and David von Oheimb. Automated Validation of Security Protocols (AVASP). Lecture slides 2005.

[2] AVISPA v1.1 User Manual 2006.

[3] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. Technical Report 39, Digital Systems Research Center 1989.

[4] Thammarat C, Kurutach W. A lightweight and secure NFC - base mobile payment protocol ensuring fair exchange based on a hybrid encryption algorithm with formal verification. Int J CommunSyst. 2019;32: e3991.https://doi.org/10.1002/dac.3991.

[5] Vanga Odelu, Ashok Kumar Das, and Adrijit Goswami. SEAP: Secure and Efficient Authentication Protocol for NFC Applications Using Pseudonyms. IEEE Transactions on Consumer Electronics 2016; 62. No. 1.:30-38.

[6] Reham Abdellatif Abouhogail, Mohammed S. Gadelrb. A New Secure and Privacy Preserved Protocol for IEEE802.11s Networks. Computers & Security Aug. 2018; 77: 745-755.

[7] Reham Abdellatif Abouhogail. A New Secure Lightweight Authentication Protocol for NFC mobile Payment. International Journal of Communication Networks and Information Security (IJCNIS) August 2019; Vol. 11, No. 2: 283-289.

[8] Hua Guo, Ya Gao, Tongge Xu, Xiyong Zhange, Jianfeng Y. A secure and efficient three-factor multi-gateway authentication protocol for wireless sensor networks. Ad Hoc Networks 2019; 95: 1-16.

[9] Sriramulu Bojjagani, V.N. Sastry. A secure end-to-end proximity NFC-based mobile payment protocol. Computer Standards & Interfaces 2019 Oct.; 66: 1-21.

[10] Michail Sidorov, Ming Tze Ong, Ravivarma Vikneswaran, Junya Nakamura, Ren Ohmura and Jing Huey Khor. Ultralightweight Mutual Authentication RFID Protocol for Blockchain Enabled Supply Chains. IEEE ACESS. DOI 10.1109/ACCESS.2018.2890389, IEEE Access.

[11] Reham Abdellatif Abouhogail. Improving the Handoff Latency of the Wireless Mesh Networks Standard. International Journal of Security and Its Applications 2016; 10: 73 -86.

[12] Reham Abdellatif Abouhogail. Fast Handover with Privacy Preserving Authentication Protocol for Mobile WiMAX Networks. International Journal of Security and Its Applications 2014; 8:361-376.

[13] Pascal Lafourcade, and Maxime Puys. Performance Evaluations of Cryptographic Protocols Veri_cation Tools Dealing with Algebraic Properties. International Symposium on Foundations and Practice of Security 2016.

[14] David A. Basin, Sebastian Modersheim, and Luca Vigano. Ofmc. A symbolic model checker for security protocols 2005; Int. J. Inf. Sec., 4(3):181- 208

[15] Mathieu Turuani. The CL-Atse Protocol Analyser. In Frank Pfenning, editor, 17th International Conference on Term Rewriting and Applications - RTA 2006 Lecture Notes in Computer Science, 4098 of LNCS: 277-286. Springer, August 2006.

[16] C.J.F. Cremers. The Scyther Tool: Verification, falsification, and analysis of security protocols. In Computer Aided Verification, 20th International Conference, CAV, 5123/2008 of LNCS, Springer, 2008: 414-418.

[17] Meier S., Schmidt B., Cremers C. Basin D. The TAMARIN Prover for the Symbolic Analysis of Security Protocols. In: Sharygina N., Veith H. (eds) Computer Aided Verification. CAV; 2013. Lecture Notes in Computer Science, vol 8044. Springer, Berlin, Heidelberg

[18] Cremers, C.J.F. The Scyther tool: Verification, falsification, and analysis of security protocols. Paper presented at CAV 2008. LNCS. Gupta, A., Malik, S. (eds.), vol. 5123, 414–418. Springer, Heidelberg 2008.

[19] B. Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In Proceedings of CSFW'01: 82-96. IEEE Comp. Soc. Press 2001.

[20] Bruno Blanchet, Ben Smyth, Vincent Cheval, and Marc Sylvestre. Cryptographic Protocol Verifier User Manual and Tutorial. May 16, 2018.

[21] Luca Vigan. Automated Security Protocol Analysis with the AVISPA Tool. Electronics notes in theoretical computer Science 2006; 155: 61–86.

[22] Ronan Saillard, Thomas Genet. CAS+. March 21, 2011. Available at:

[23] http://people.irisa.fr/Thomas.Genet/span/CAS_manual.pdf. [accessed 18.08.2019].

[24] Pisarev I.A., Babenko L.K. Registration protocol security analysis of the electronic voting system based on blinded intermediaries using the Avispa tool. In Proceedings of Trudy ISP RAN; 2018; 30; 4 155-168; Russia: ISP RAS

[25] Sheng Ding, Jin Cao, Chen Li, Kaifan, and Hui Li. A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. IEEE Access 2019; 7: 38431- 38441.

[26] Li Gong, Roger Needham, and Raphael Yahalom. Reasoning about belief in cryptographic protocols. In Proceedings of 1990 IEEE Symposium on Research in Security and Privacy; 1990 May 234–248. IEEE Computer Society.

[27] Paul F. Syverson and Paul C. van Oorschot. A unified cryptographic protocol logic. CHACS Report. 1996. NRL Publication. pp. 5540–227, Naval Research Lab.

[28] Ben Smyth. "FORMAL VERIFICATION OF CRYPTOGRAPHIC PROTOCOLS WITH AUTOMATED REASONING". Ph.D. thesis. University of Birmingham. March 2011.

[29] Colin Boyd and Wenbo Mao. On a Limitation of BAN Logic. Springer-Verlag, 1993: Pp.240-247.

Authors' Profiles

Dr. Reham Abdellatif Abouhogail is currently working as an associate professor researcher at the National Institute of Standards (NIS), Egypt since 2015. She graduated from Faculty of Engineering Ain Shams University in 2000, she obtained Master degree in electronics and communications from Cairo University in 2004. She obtained Ph.D degree from Faculty of Engineering Ain Shams University in 2009. She has 18 years of experience of research. Her area of research includes design and analysis of security protocols and wireless networks security systems. She has published many research papers in international journals and in international conferences.

How to cite this paper: Reham Abdellatif Abouhogail, "A Comparative Analysis of Tools for Testing the Security Protocols", International Journal of Information Technology and Computer Science(IJITCS), Vol.11, No.12, pp.30-37, 2019. DOI: 10.5815/ijitcs.2019.12.03