Proxy Base Station based Authentication Protocol for Broadband Wireless Network

Fuden Tshering
Indian Institute of Technology Roorkee
Roorkee-247667, India

Prachi Deshpande
Indian Institute of Technology Roorkee
Roorkee-247667, India

S.C.Sharma, PhD.
Indian Institute of Technology Roorkee
Roorkee-247667, India

Anjali Sardana, PhD.
Indian Institute of Technology Roorkee
Roorkee-247667, India

ABSTRACT
The fourth generation technology of broadband wireless networks i.e. WiMAX (Worldwide Interoperability for Microwave Access) became popular due to its features like high speed internet access, large coverage area and interoperability for different type of devices. Non-Line of-sight propagation with lower frequency improvement makes WiMAX vulnerable to various security threats. Hence, authentication and authorization are used for protecting network from various attacks.
Although there are standard authentication protocols in IEEE 802.16, but still WiMAX is vulnerable to attacks such as replay attack, DoS (denial of service attack), interleaving attack etc. In this paper, an exhaustive analysis of existing solutions in standard PKMv2 (privacy key management version 2) protocol is presented.
The Proxy Base Station based authentication protocol addresses the major attacks namely DoS attack, interleaving attack, replay attack and downgrade attack. With the introduction of PS (proxy base station), the task of validation is distributed between the PS and BS (base station), it resolves the DoS attack due to the resource exhausting validation procedure [23]. Our proposed authentication protocol is modeled and verified on CPN (Colored PetriNet) tool (version 3.0.2)[1, 2] with and without intruder and compared with PKMv2 standard protocol. The state space analysis report for standard verification parameters shows that our proposed protocol satisfies the desired properties of liveliness and fairness with negligible overheads and it is secure and efficient.

General Terms
Security, Wireless, Algorithms, Networks

Keywords
WiMAX, Authentication, Proxy, Base station, protocol, Privacy and key management

1. INTRODUCTION
WiMAX can be described as a telecommunications technology aimed at providing wireless data over long distances in a variety of ways, from point-to-point links to full mobile cellular type access. It is based on the IEEE 802.16 standard [3]. In 2005, the IEEE 802.16e [4] was released to address the mobility which enables MBs (mobile stations) to handover between BSs while communicating. This standard is often called "Mobile WiMAX". The IEEE 802.16 currently employs the most sophisticated technology solutions in the wireless world, and correspondingly it guarantees performance in terms of covered area, bit-rate, and quality of service. There is big need of securing the WiMAX environment so that it can be delivered in public successfully. In wired networks, various approaches exist for these attacks. But they can't be adopted for IEEE 802.16e wireless network [5-12]. WiMAX is susceptible to the attacks such as replay, DoS and MITM (man in the middle) attacks. In replay attack the authorization request is replayed multiple times to the BS, which will make the BS ignore the SS (subscriber station). Owing to the mobility of wireless network, in DoS attack, if a SS sends a lot of false authorization requests to a BS, the BS will use all its resources to calculate whether the certificate is correct or else. This will cause DoS, as BS will not be able to serve any SSs anymore. The MITM is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them. It makes victims to believe that they are talking directly to each other over a private connection, where in fact the entire conversation is controlled by the attacker.

Section 2 describes the brief literature review of the related work. Section 3 describes the design details of proxy BS (base station) based authentication protocol for IEEE 802.16e. Section 4 describes the experimental details of the proposed protocol. Results are discussed in section 5. Section 6 concludes the whole work and gives pointers for future work.

2. LITERATURE REVIEW
Message replay attack is one of the most common attacks on authentication and authenticated key establishment protocols. If the messages exchanged in an authentication protocol do not carry appropriate freshness identifiers, then an intruder can easily get himself authenticated by replaying messages copied from a legitimate authentication session. MITM attack is another classic attack and is generally applicable in a communication protocol where mutual authentication is absent. Other familiar attacks include the parallel session attack, reflection attack, interleaving attack, attack due to type flaw and attack due to misuse of cryptographic services. Detailed discussion and examples of these attacks can be found in [13]. PKMv2 is the standard authentication protocol proposed to overcome flaws of PKMv1 (privacy key management version 1) protocol [14].The PKMv2 model is a four step protocol and uses 3-way authentication. Figure 1 shows the PKMv2 model. PKMv2 is based on alternating nonce approach as proposed in 802.16e. Although it solves some of the issues in PKMv1, yet a number of these problems

remain unresolved. It implements mutual authentication of SS and BS using individual X.509 certificates, CerSS and CerBS, respectively.

The incorporation of interchanging nonce helps to link subsequent messages as well as to counter intrusion activity as nonce is random and cannot be easily predicted. The SSID (SS identifier) unique for each SS in the network, is assigned in MSG3 (message 3). Digital Signatures of BS, as in MSG3, enhance the authenticity of message and the SAID (security association identifier) determines the selected security association. An additional fourth step has been introduced in which, the SS acknowledges the authorization reply message with BSs nonce from MSG3 and SS address. Both these parameters encrypted using the authorization key (EAK (NB, SSAddr)) [14].

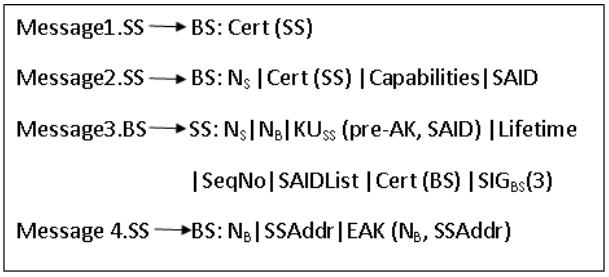

Fig 1: PKMv2 protocol

The authors in [15, 16, 17, and 18] have addressed the DoS/Reply attacks. They require a reasonable modification to the standards. In [16], computing and analyzing the value of γ (gamma) increases the complexity. Although [17] counters DoS effectively, it has increased the number of message exchanged thus affecting the performance. In [19], the authors have proposed completely new protocol for authentication and authorization process which requires complete modification to the standard. In [19], the author solves the key space vulnerability issue. However experiments are required to validate the behaviour and performance of this solution. Also, the author in [19] solved the downgrade attack but it may create another issue of DoS. So this solution cannot be considered to operate satisfactorily. The author in [20] described that ECC is better than RSA. In [21, 22], the authors have solved the initial network entry vulnerability issue but still it is prone to other attacks. Table 1 shows the comparison of different solutions.

Our proposed proxy BS based authentication protocol addresses the following issues:

- DoS attack
- Downgrade attack
- Interleaving attack (MITM)
- Replay attack

3. PROPOSED SOLUTION

Proxy base station is placed in between SS and BS. SS sends authentication and authorization messages to BS but PS receives them first and validates theses messages. After validation PS sends the messages to BS. PS has validated authorization message sent by SS then BS just sends authorization reply after reading request. Acknowledgement message is sent by SS to BS and afterwards the key exchange between BS and SS is performed. Thus further communication is enforced. The SSs cannot overwhelm the BS with too many rogue requests due to the presence of PS. Even if the SSs overwhelm the PS with rogue requests, the BS would continue providing services to the authorized SSs. PS handles the authorization validation step which gives decreased computational overhead to BS. The possibility of computational overhead causes DoS attack is neutralized due to decrease in computational overhead of BS. Due to introduction of PS between SS and BS the more number of messages are also introduced resulting in increased response time from BS to SS. But the protocol can handle Dos attack effectively. Here the BS will not experience any unnecessary computation and can continue providing services to the authorized SS. Although, there is an overhead of adding the proxy station, which increases the number of messages communicated and also the response time of the BS to the SS, it's prepared for the worst DoS attack. Figure 2 shows the design of proposed protocol. To implement this approach in real time, a major amendment in the standard and hardware is required.

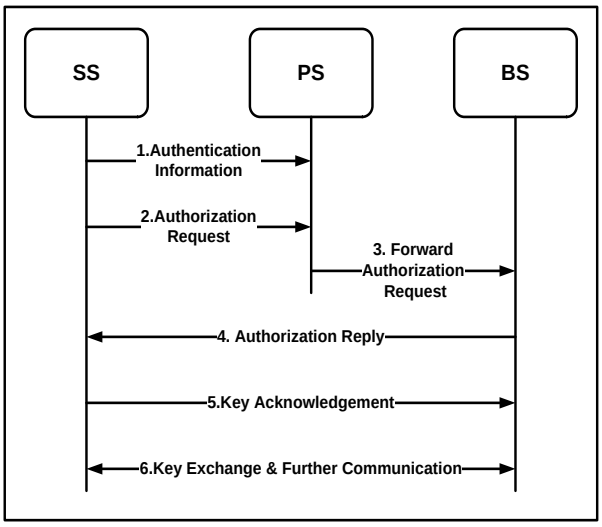

Fig 2: The design of the proposed protocol [23]

4. EXPERIMENTAL DETAILS OF THE PROPOSED PROTOCOL

The model verification is done with and without intruder part. CPN tool is used for modeling separate pages (subnets) for the SS, the BS, the PS and the intruder part.

4.1. PKMv2 authentication protocol modeling on CPN tool

4.1.1. Modeling PKMv2 without intruder

The following section elaborates the hierarchical CPN with separate pages (subnets) for the SS, the BS and the intruder part.

4.1.1.1. The top-level model

Figure 3 shows the CPN top-level model for PKMv2 with no intruder. It presents the PKM protocol in a modular way. The model of the protocol is constructed by using sub-models of its agents. In CPN, this is implemented by using substitution transitions. First, the messages exchanged between the protocol entities are focused. At this level, protocol entities are modeled as transitions. The two transitions SS and BS represents the SS and BS of PKMv2 protocol. Here the place A represents the authentication information message, place B represents the authorization request, place C represents

authorization reply message and place D represents key acknowledgement message.

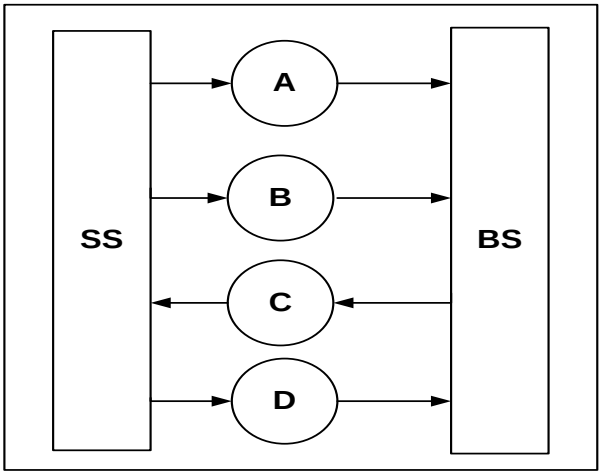

Fig 3: CPN top-level model for PKMv2 with no intruder

4.1.1.2. Defining the top-level substitution transitions

The detailed models of the SS and the BS are explained in Figure4 and 5 respectively. The CPN model of the SS contains three subnets: one models the subtask of SS initiating a protocol run in step 1, the second step sending authorization request and the third one receiving the authorization reply and acknowledging the reply. In this page, SS sends the authentication information message through SendMSG1 place. The transition GenerateMsg2 generates the authorization message, using the three places for certificate, nonce and other items such capabilities and SAID, and sends it to BS through SendMSG2 place. The authorization reply is received at place SendMSG3 place which is decrypted using the public key of BS.

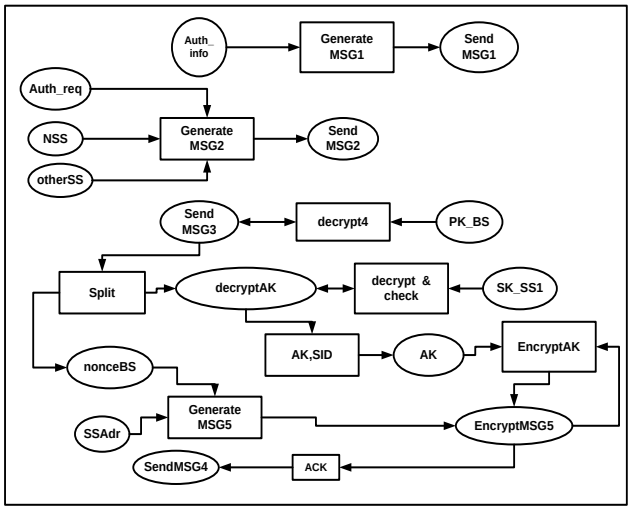

Fig 4: SS page

Then the validation of this message is done. After validating the message the AK (acknowledgement) is conceived by decrypting the encrypted AK part within received message. The nonce and AK key are used by SS to generate message 4.

The transition Encrypt AK shows the encryption of the message plain message generated at transition GenerateMSG4. The sendMSG4 place is the key acknowledgement message. The CPN model of the BS contains three subnets: receiving the authentication information, protocol run in step 1, the second step receiving authorization request, the third one is sending the authorization reply and receiving acknowledgement.

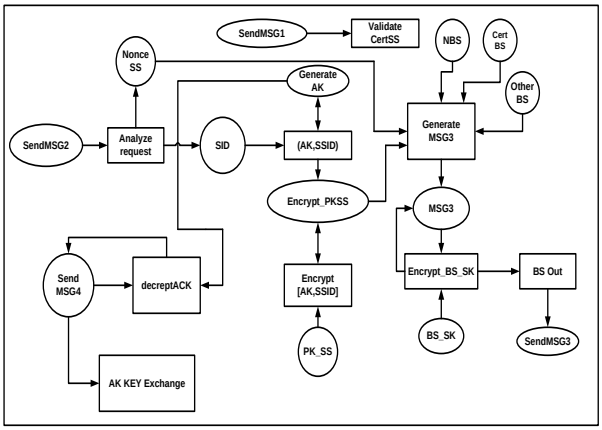

Fig 5: BS page

In this page, place SendMSG1 is used to receive the authentication information and the certificate of SS is validated. The BS receives the authorization request through SendMSG2 place, it directly analyses the request for validation and then according to the SSs capabilities it generates AK and encrypts it with PKSS (public key of SS) using the key from PK SS place.

Then the transition GenerateMSG3 generates the message. This message is encrypted at transition encrypt BSSK using the private key of BS from BSSK place. This message is send to SS through SendMSG3 place. Through place SendMSG4 the BS receives the key acknowledgement message and is decrypted at transition decryptACK using the key provided by GenerateAK place. If decrypted successfully the AK is exchanged successfully.

4.1.2. Modeling PKMv2 with intruder

It is required to consider a large number of cases to analyze a cryptographic protocol by adding a general intruder model. This makes the analysis task infeasible in many situations. Hence, the idea is to find the set of modified output data that doesn't affect the acceptance of the data by the legitimate protocol users. Then, only this set of data is to be used in the analysis. This step helps us to identify the vulnerable points in the protocol and to adaptively model the intruder.

The inputs to this automated step are the variables that the intruder can modify, and the variables which the legitimate user will check. The simulation will specify the set of vulnerable data which can be modified by the intruder and still will be accepted by the legitimate stations. In order to add the intruder to the model, one must extend the CPN modeling declarations.

4.1.2.1. Top-level model with an intruder

Figure 6 shows the top level model of the PKMv2 protocol with an intruder. The substitution transition IR represents the intruder. The intruder is modeled as a separate entity that controls the communication channels between the protocol entities. Thus, it intercepts the exchanged messages and stores them for future use. Then, it attempts to decrypt the encrypted portions of the intercepted messages. Finally, it attempts to

modify the message contents, or even to generate new messages to replace the intercepted ones.
Here the messages A,B,C,D are intended to be exchanged between the SS and the BS but the intruder intercept, store, modifies and forwards the spoofed messages. The places A, B, C and D shows the legitimate messages sent by SS and BS and the places IA, IB, IC and ID shows the modified messages sent by the intruder to get the control over communication channel between SS and BS.

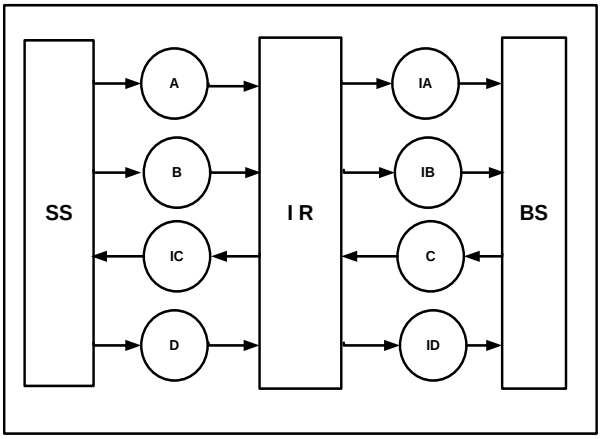

Fig 6: CPN top-level model for PKMv2 with intruder

4.1.2.2. Defining the intruder substitution transition

The intruder substitution transition (IR in Figure 6) is defined by the subpage intruder shown in Fig 7. The intruder first stores the fields of the intercepted message. Then, it tries to decrypt the cipher using one of the public key stored in its database. Finally, the intruder forms a new message to be sent in place of the Intercepted one. This page contains four subnets. First stores and modifies the authentication information message. Second, stores and modifies the authorization request stage. Third, receives the authorization reply message and forwards the modified one to SS and finally accepts the key acknowledgement. Here the intruder receives the authentication message through sendMSG1 place which it stores and forwards the desired message to BS through sendIMSG1 place. The authorization request is received at sendMSG2, the intruder stores and modifies this message and sends to BS through sendMSG2. The sendMSG3 is the authorization reply message received from BS and forwarded the modified one to BS through place sendIMSG3. The place sendMSG4 is the key acknowledgement message received from SS and sendIMSG4 is the modified message send to BS.

4.2. Proposed Protocol

4.2.1. Modeling the proposed protocol without intruder

The proposed protocol is modeled in a hierarchical approach. The following sections describe the hierarchical CPN with separate pages (subnets) for the SS, the BS and the PS.

4.2.1.1. The top-level model

It presents the model of proposed protocol in a modular way. Thus, the model of the protocol is constructed by using sub-models of its agents. In CPN, this is implemented by using substitution transitions. First, the messages exchanged between the protocol entities are focused. At this level, protocol entities are modeled as transitions. Figure 8 shows a top-level model of the proposed protocol. The three transitions SS, PS and BS represent the SS, PS and BS of the proposed protocol.

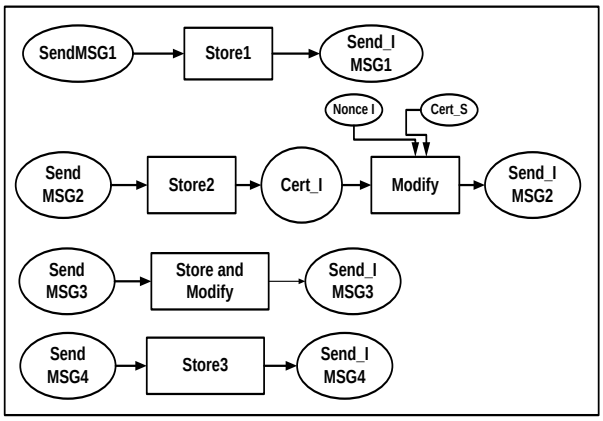

Fig 7: Intruder page

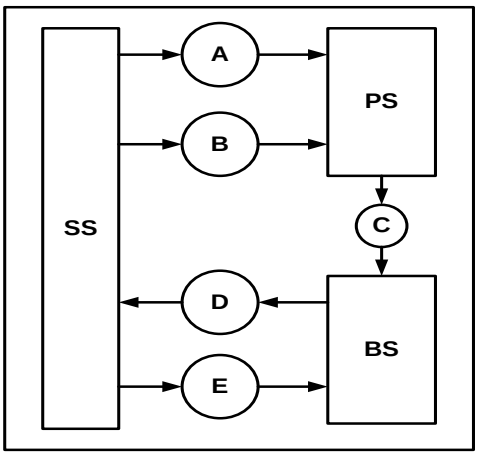

Fig 8: CPN top-level model for proposed scheme.

Here the place A represents the authentication information message, place B represents the authorization request, place C represents forward authorization request message, place D represents the authorization reply message and place E represents key acknowledgement message.

4.2.1.2 Defining the top-level substitution transitions

Here the models of the SS, the PS and the BS are considered in detail. The CPN model of the SS contains three subnets: one models the subtask of SS initiating a protocol run in step one, the second step sending authorization request and the third one receiving the authorization reply and acknowledging the reply. In this page, SS sends the authentication information message through SendMSG1 place. The transition GenerateMsg2 generates the plain authorization message, using the four places for certificate, nonce, timestamp and other items such capabilities and SAID, and the transition Encrypt SK encrypts this plain message using the private key of SS received from place SK SS.
Then SS sends encrypted authorization request message to PS through SendMSg2 place. The authorization reply is received at place SendMSG3 place which is decrypted using the public key of BS and then the validation of this message is done. After validating the message the AK is conceived by

decrypting the encrypted AK part within received message. The nonce and AK key are used by SS to generate message 4. The transition EncryptAK shows the encryption of the message plain message generated at transition GenerateMSG4. The sendMSG4 place is the key acknowledgement message.

Figure 9 shows the CPN model of the PS. It contains three subparts: receiving the authentication information in step one, the second step is receiving authorization request, and the third one is forwarding the authorization request after decrypting and validating the authorization request message.

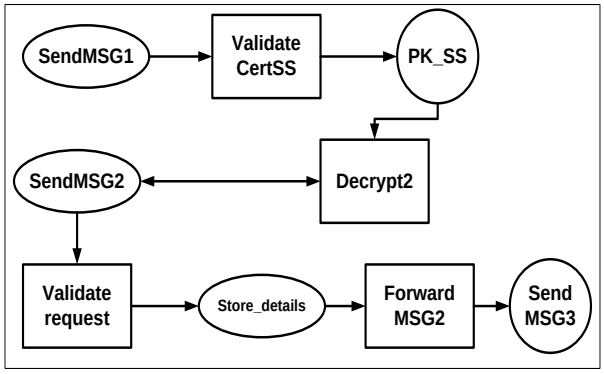

Fig 9: PS page

In this page, place sendMSG1 is used to receive the authentication information and the certificate of SS is validated. The PS receives the authorization request through sendMSG2 place and decrypts this message using the public key of SS conceived after validating certificate from place PK SS. Then, the PS analyses the request for validation. After analysis, it forwards the decrypted authorization request message to the BS through the place SendMSG3.

The CPN model of the BS (Figure10) contains three subnets: receiving the authorization request forwarded by PS, the second one is sending the authorization reply to SS and the last one is receiving acknowledgement from SS. In this page, the BS receives the authorization request through sendMSG3 place, it directly analyses the request and then according to the SSs capabilities it generates AK and encrypts it with public key of SS along with SSID at transition Encrypt(AK,SSID) using the key from PK SS place.

Then the transition GenerateMSG3 generates the message incorporating the timestamp, nonce, certificate and other items such as AK lifetime, SAID etc.

This message is encrypted at transition encrypt BSSK using the private key of BS from BS SK place. This message is send to SS through SendMSG4 place. Through place SendMSG5 the BS receives the key acknowledgement message and is decrypted at transition decryptACK using the AK key provided by GenerateAK place. If decrypted successfully the AK is exchanged successfully.

4.2.2 Modeling the proposed protocol with intruder

The proposed protocol is tested with the intruder that is just trying to replay the earlier authorization request message. This stored message cannot be modified because it is encrypted with the private key of SS. The replayed message is easily identified by the timestamp contained in this message. Thus, the model with intruder will not reach to the final state because the PS identifies that this is a replayed message. In order to add the intruder to the model, one must extend the CPN ML declarations.

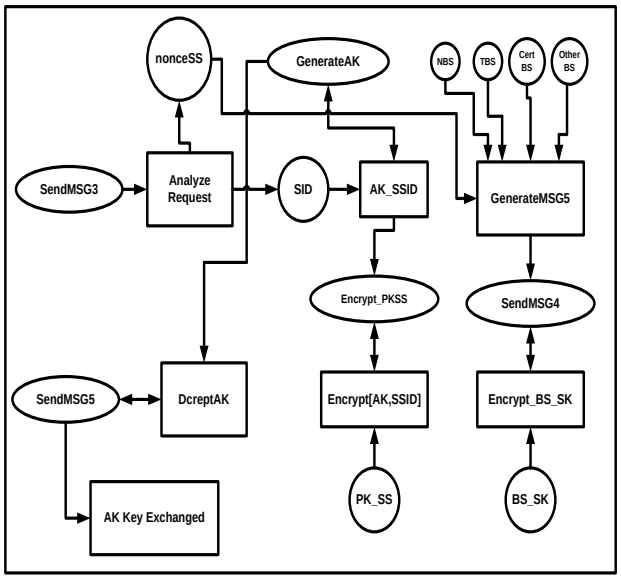

Fig 10: BS page.

4.2.2.1. Top-Level Model with an Intruder

Figure 11 shows the top level model of the proposed protocol with an intruder. The substitution transition IR represents the intruder.

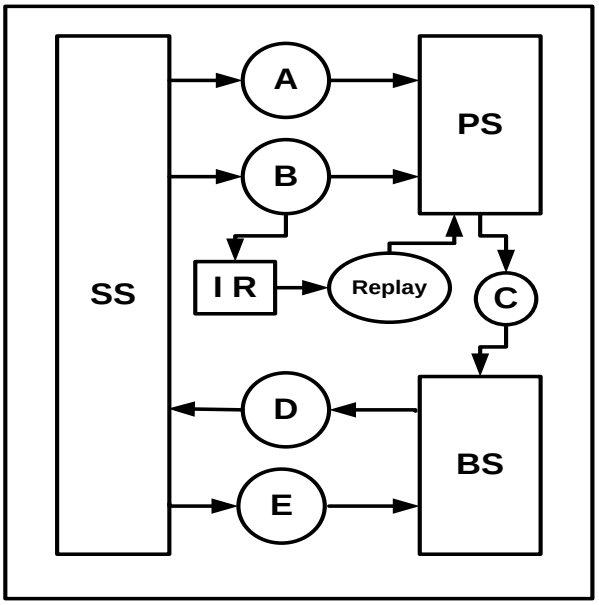

Fig 11: CPN top-level model for proposed protocol with intruder

The intruder is modeled as a separate entity that controls the communication channels between the protocol entities. It listen the authorization request message and replays them for future use and it attempts to decrypt the encrypted portions of the intercepted messages. The validation of replay message in PS page is shown in Figure12. Finally, it attempts to modify the message contents, or even to generate new messages to replace the intercepted ones. In this page, the transition IR represents the intruder which simply listen the message from

place B and replays this message to PS through the place replay. The rest of the transitions and places are as it is in the proposed model without intruder.

4.2.2.2. Replay message validation by PS

The Figure12 shows the substitution page of PS where PS is validating the replayed authorization request message in proposed protocol. Here the place SendIMSG1 represents the receiver of the message replayed by the intruder. As the replayed message is a encrypted with the private key of SS, it is decrypted with the public key of the SS.

After decrypting the message, PS validates the message, at transition named check, by checking the timestamp of the arrived message. If the timestamp of the replayed message is greater than the previous received message then it is validated as legitimate otherwise it is discarded here. Since, the message is the replayed one the timestamp will be less than the timestamp present in the record. Thus this model with intruder fails to reach the final state.

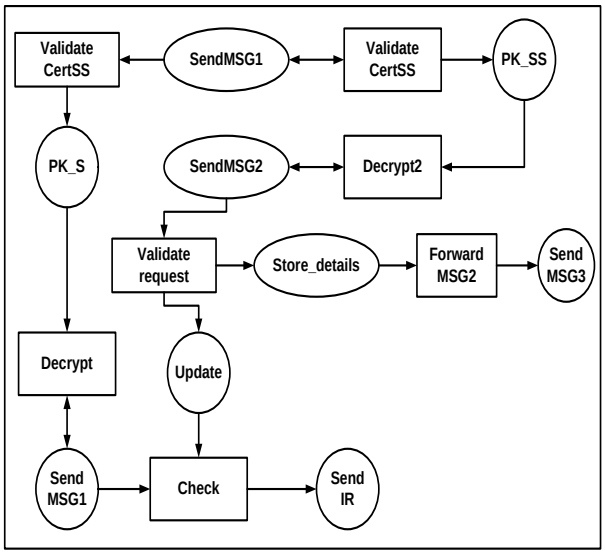

Fig 12: Validation of replay message in PS page

5. RESULTS

The standard formal verification parameters derived from the state space analysis report are:

1. Liveness Property: If the execution reaches to the final state then liveness is satisfied otherwise not.
2. Fairness: It determines whether the set of transition instances is impartial or fair.
3. Deadlock: Deadlock means the protocol will unexpectedly terminate in the case of resource accessing conflict or unlimitedly waiting for acknowledge packets [24].
4. Number of Nodes: With the introduction of intruder the number of nodes increases.
5. Number of Arcs: As the number of nodes increases the number of arcs also increases.

To analyze the state space, the report is generated using the state space tool in CPN. The report generated for the four models showing the different desired properties are to be consolidated in table 2 given in the end of paper.

From the table 2, it can observe that the even after adding the attacker to PKMv2 model, the intruder reaches to the final state successfully. There is no deadlock and the liveness property is satisfied. But the number of arcs and nodes are increased almost to the twice of model without intruder. So the only way to detect the intrusion is by noticing the increased number of nodes and arcs in the state space results. This is because the authorization request message sent by the SS is open to everyone and can be modified easily.

Thus without the knowledge of SS and BS the intruder can easily compromise the privacy of the communication channel. Hence the intruder goes undetected in the standard PKMv2 protocol. In the case of the proposed protocol model there is no deadlock and the fairness and liveness properties are satisfied. With introduction of PS in proposed protocol the number of nodes and arcs are increased as compared to standard PKMv2 protocol.

As observed from the table 2, the modeling of proposed model with intruder does not increase the number of nodes and because the replied message was unable pass through the validation at PS page. So there is unexpected termination which results to deadlock and liveness property is not satisfied. Hence the intruder fails to compromise the network and reach the final state.

6. CONCLUSIONS AND FUTURE WORK

6.1 Conclusions

The standard PKMv2 authentication protocol is vulnerable because the messages exchanged between the SS and BS is not secured. To solve this issue a proxy BS based authentication protocol is proposed, which is efficient in tackling the various security threats such as replay attack, DoS (denial of service) attack, interleaving attack and downgrade attack.

The proposed protocol is more secure against the intruder than the standard PKMv2 protocol. The numbers of messages exchanged are almost same because the message 3 in proposed protocol is openly communicated through secured network. Also, in the proposed scheme the BS station can provide better quality of service as compared to the previous one because the task of authorization is distributed among PS and BS. Hence our proposed protocol is more robust against the attacks.

6.2 Future Work

In future, it is intended to work towards the implementation of the protocol in real-time environment and to use ECC cryptography which is more efficient than RSA cryptography.

7. REFERENCES

[1] AIS group, Eidhoven University of Technology, The Netherlands (2011)http://cpntools.org.

[2] Al-Azzoni, D. G. Down and R. Khedri, "Modeling and verification of cryptographic protocols using Colored PetriNet and design/CPN," Proceedings of MOMPES05:1-28(2005).

[3] WiMAX Forum, Fixed, Nomadic, Portable and Mobile Applications for 802.16-2004 and 802.16e WiMAX Networks (Nov.2005).

[4] IEEE 802.16-2005, IEEE standard for Local and Metropolitan Area Networks- Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, IEEE Press (2005).

[5] Anjali Sardana and R. C. Joshi, "Simulation of Dynamic Honeypot Based Redirection to Counter Service Level

DDoS Attack", Lecture Notes in Computer Science: 4812,259-262(2007).

[6] Anjali Sardana, K. Kumar and R.C. Joshi, "Detection and Honey pot Based Redirection to Counter DDoS Attacks in ISP Domain", Third International Symposium on Information Assurance and Security (IAS 2007), 191-196(2007).

[7] Anjali Sardana and R. C. Joshi, "Honeypot Based Routing to Mitigate DDoS Attacks on Servers at ISP Level", International Symposiums on Information Processing (ISIP2008),505-509(2008).

[8] Anjali Sardana and R. C. Joshi, "Autonomous Dynamic Honeypot Routing Mechanism For Mitigating DDoS Attacks in DMZ", 16th IEEE International Conference on Networks (ICON 2008),1-7(2008).

[9] Anjali Sardana and R. C. Joshi, "An Auto Responsive Honeypot Architecture For Dynamic Resource Allocation and QoS Adaptation in DDoS Attacked Networks", Journal of Computer Communications: 32(12)1384-1399(2009).

[10] Anjali Sardana and R. C. Joshi, "Dual-Level Defense For Networks Under DDoS Attacks", Proceedings of the ACM Symposium on Applied Computing (SAC 2010):733-734(2010).

[11] Anjali Sardana and R. C. Joshi, "Dual-Level Attack Detection, Characterization and Response for Networks under DDoS Attacks", International Journal of Mobile Computing and Multimedia Communications (IJMCMC):3(1), 1-20(2011).

[12] Anjali Sardana and R. C. Joshi, "Dual-Level Attack Detection and Characterization for Networks under DDoS", International Conference on Availability, Reliability, and Security (ARES 10):9-16(2010).

[13] Wenbo Mao, "Modern Cryptography: Theory and Practice", Pearson Education, Prentice Hall PTR (2004).

[14] A. Altaf, M. Y. Javed, A. Ahmed, "Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005", Proceedings of 9th International Conference on software Engineering, Artificial Intelligence., Networking and Parallel/Distributed Computing:335-339(2008).

[15] S. Xu, M. Matthews, C. T. Huang, "Security Issues in Privacy and Key Management Protocols of IEEE 802.16", Proceedings of 44th annual southeast regional conference, Melbourne, Florida: 113-118(2006).

[16] A.Altaf, R. Sirhindi and A. Ahmed, "A Novel Approach against DoS Attacks in WiMAX Authentication using Visual Cryptography", Proceedings of 2nd International Conference on Emerging Security Information, System and Technologies, Secureware, France: 238-242(2008).

[17] H. Dong and W. Yan, "Secure Authentication on WiMAX with Neural Cryptography", Proceedings of International Conference on Information Security and Assurance,366-369(2008).

[18] Y. Yang and R. Li, "Toward WiMAX Security", in Proceedings of Computational Intelligence and Software Engineering, Wuhan, China:1-5(2009)

[19] F.Liu and L.Lu, "A WPKI-based Security Mechanism for IEEE 802.16e", Proceedings of Int. Conference on Wireless Communication, Networking and Mobile Computing: 14(2006).

[20] M. Habib et.al, "Performance of WiMAX Security Algorithm: The Comparative Study of RSA Encryption Algorithm with ECC Encryption Algorithm", Proceedings of International Conference on Computer Technology and Development (ICCTD09), Kota Kinabalu, Malaysia:108-112 (2009).

[21] T. Han et.al.,"Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions," Proceedings of 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, Atlanta:828 833(2008).

[22] F. Tshering and Anjali Sardana, "A Review of Privacy and Key Management Protocol in IEEE 802.16e", Int. Journal of Computer Applications, Published by Foundation of Computer Science: 20(2)2531(April 2011).

[23] F. Tshering and Anjali Sardana, "A Proxy Base Station based Authentication Protocol for IEEE 802.16e," Proceedings of IEEE ICRTIT 2011 Conference (June 2011).

[24] H.Dong and W.Yan, "Secure authentication on WiMAX with neural cryptography", Proceedings of international conference on information security and assurance, 366-369(2008).

Table 1: Comparison of different solutions

Sr.	Solution	Issues addressed	Advantage	Disadvantage
1.	Nonce[15]	Denial of Service	Synchronization not required	Unable to Check freshness the Of message
2.	Timestamp[15]		Prevents simple replay attack	Requires the Time synchronization
3.	Timestamps Together with Nonce[16]		Prevents interleaving attack	Difficult to consider the value of gama (γ)
4.	Visual cryptography For preauthentication [24]		Successfully avoids the Request from rougue SS	Increases the computational overhead by introducing TTP server
5.	ECC[20]	Cryptographic algorithm Computational efficiency	ECC requires less key size and computation	Requires modification In the standards.
6.	Diffie-Hellman key Exchange[21]	Initial network entry	Provides key to secure the messages	Vulnerable to man in the middle attack
7.	Proxy based station Based authentication Protocol [23]	--	Less computational over head for BS	Increases the response time of BS.

Table 2: Analysis of State Spaces

Approach	Fairness	Dead Lock	Liveness	No. of nodes	No. of arcs
PKMv2 without intruder	**Yes**	**No**	**Yes**	**57**	**98**
PKMv2 with intruder	**Yes**	**No**	**Yes**	**92**	**165**
Proposed Protocol without intruder	**Yes**	**No**	**Yes**	**44**	**55**
Proposed Protocol with intruder	**Yes**	**Yes**	**No**	**20**	**27**