Formal Verification of WiMAX Protocol Using Petri Nets

[1]Hafiza Samavia Kaukab, [2]Rao Sohail Iqbal, [3]Furhan Ashraf, [4]Ghulam Mujtaba,
[5]Muhammad Usman Saleem, [6]Abdul Rehman
[1,2,3, 4,5,6]Dept. of Computer Science, GC University Faisalabad, Punjab, Pakistan

Abstract
WiMAX technology is growing rapidly and has much social influence on people (user) which offers high-speed internet service and also ignores Wi-Fi interrupts, therefore, it is assumed that it has some security issues like the man in the middle attack, DoS attack, Rouge Base attack etc. In this era of technology the reliability enhancement is very important and demand for user satisfaction. Formal methods are the mathematical language and identify the possible errors of the system at the conceptual modeling phase. These attacks can be identified at the conceptual modeling phase and the developed system maybe attack free and error free. Petri nets is the graphical representing language of the system which is under development and it also covers all the functionalities of the system. Petri nets is mostly used by the researchers for formalization purposes. In this research, the Diagram of WiMAX protocol will be first analysed and then its equivalent Petri net model will be developed which will cover all the working of the system. Finally, the model will be verified by designing a reachability tree. This will make the WiMAX system formally verified and we can then say the WiMAX system is formally verified.

Keywords
WiMAX, Man in the Middle Attack, DoS Attack, Rouge Base Attack, Formal Methods, Petri Nets, Reachability Tree.

I. Introduction

WiMAX is a wireless digital communication system that eliminates Wi-Fi interruptions, therefore, it is assumed that its security scheme was challenged by the number of attacks [17].
In the development of fast communication firstly 2G technology was introduced in the late 1990s that allow the users to make calls and messages to communicate with each other. Then 2.5G technology was developed which was a bit faster than 2G and it works with GPRS, E-Mail, and Web Browsing etc. [7]. After that 3G technology was introduced which was very fast as compared to its previous versions and it also provides high bandwidth. The latest technology is the 4th generation which is 4G LTE which provides a bandwidth of 100 Mbps-1Gbps, WiMAX has great importance in 4G technology [7]. 4G includes two items LTE and WiMAX 2 which was adopted in 2011, this technology fixed the issues in wireless networks by providing comprehensive IP solution anywhere [5].
The old fashioned wired technology is replacing with Wireless communication technology today [15]. WiMAX is well known wireless communication technology that provides high-speed internet access around 70 Mbps at the area of 30 to 40 miles [8]. Most wireless networks are restricted to open interference and Wi-Fi is becoming remote innovation and it has a security concern. So there is a need for strong security management for the protection of WiMAX from threats [1].
Formal methods are used by most of the researchers to manage the security issues e.g. privacy, authentication, and non-suspension of validity guarantee [17]. There is no formal explanation for WiMAX but the goals which are offered for 4G and WiMAX are defined [6]. The system of mobile communication is still providing a solution to 3G system problems and it also provides high-quality new services to the system [6]. There are some formal methods for wireless communication have been developed yet and these methods are based on analysis and validation [18].
Formal methods have many languages but most of the researchers used Petri Nets for the formalization of the system. Petri net is a place/transition net which describes the system [2][23]. Petri nets is a graphical representation of the system which is used further for verification purposes [23].

II. Related Work

As increasing demand for mobile internet and wireless multimedia applications has encouraged the development of wireless broadband technology in recent years. WiMAX Air Interface Using Multiple Access is the most accessible method for batter multipath performance[18]. WiMAX firstly described in IEEE 802.16-2004 standard which provides the mail to WMAN network [19].
Safety features e.g. privacy, confirmation of payloads and privacy of keys between network components are analysed in [22] and resulted that the use of first protocol is a way to ignore and evaluate multiple paths in a deceive fashion by using different types of search engines and it will also be in the result to increase the efficiency of routing protocol [22].
Shaddad .R, et al (2014) resulted in his research that as WiMAX technology provides mobility in broadband wireless, therefore, it is very useful by open-air media as a broadcast channel. This is the reason for high-security risks for all wireless networks. These risks may be in the type of privacy loss, data loss on both user and provider side, unauthorized use and internal attacks. Shaddad, R. et al (2014) defined a sublayer by the help of 802.16 Quality Medium Access Control (MAC) which is below the layer and this sublayer is used as security sublayer certification, key formation as well as information encryption [19].
It is presented in [3] that the security sub-layer has two protocol components: the first one is an encapsulation protocol used for the encryption of the packet data and the second component is confidentiality and key management (PKM) protocol which is used to provide secure distribution of key data (SS). [9] Proposed that Formal analysis of PKMv1 and PKMv2 are done by a tool Scythe to extract threat that might exist in the protocol. This study helps us to begin the analysis and assessment of security goals and also proposed the expected modifications to ensure formally secure protocol.
The errors or threats in WiMAX protocol might be one of the type man in the middle attack, initial network entry [22], DoS attack, Rouge Base attack [15], privacy loss, and data loss as well as providers, unauthorized use [19], transfer of unauthorized messages [14] etc.
There were some basic semantics and definition about the Petri nets are given in [2][23] that a Petri net is a graphical representation of the system which consists of places, transitions, and arcs. Petri

net is introduced by Carl Adam Petri in 1962 and it is considered as a formal mathematical language. Petri net is used to formalize the model under development to detect the errors and deadlocks of the system before its implementation [16]. There are two aspects of Petri nets are presented in [16] which are considered as the key for the Petri net acceptance, the first aspect is the model provide the knowledge about the system behavior and the other aspect is that the system shows the visualization of the system and state changes of the system.

Petri net is used in [2],[4],[10-13],[20] for formalization of different systems and models, this method of formalization is motivated us to make WiMAX formalize.

III. Background

This section will provide the basic knowledge about WiMAX, Petri nets and reachability tree which is used for the formalization of the system.

A. WiMAX Block Diagram

WiMAX block diagram shows two different parts of the system. First is the transmitter off and the other part is the receiver of the data. There is communication which allows these parts of the system to communicate with each other. The first part of the diagram is the transmitter side which contains the combination of different functions and devices which can take part in the transmission of the right data to the right destination. The second part of the diagram is the receiver side and also contains the functioning devices that can assure of the data which is received is right. The interface that makes the communication possible between these parts is said to be a channel. We can say the working in the transmitter side is the wrapping the data and the working on the receiver side is unwrapping of the data. The block diagram of WiMAX is given below.

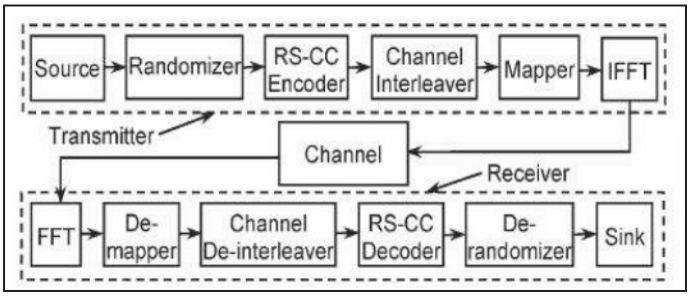

Fig. 1: Block Diagram of WiMAX.

Block diagram of WiMAX shown in fig. 1. The fig. shows two main parts as discussed above one is a transmitter and the other is the receiver. The transmitter sends the data and the receiver receives the data. This communication can be possible through an interface which is labeled as a channel in the diagram. WiMAX system has sequence wise functions that the functions in the transmitter side came, at last, they came first in the receiver side. This can be said that is a wrapping based function, that what is wrapped in transmitter it will be unwrapped in the receiver side. These parts of the system can be shown separately that can help the reader to understand the individual working of the system.

B. Transmitter of Data

The first part that is the sender side of the system which transmits the data and this part is shown in the figure below. This figure shows the individual working on the transmitter side of the system. The diagram is given below.

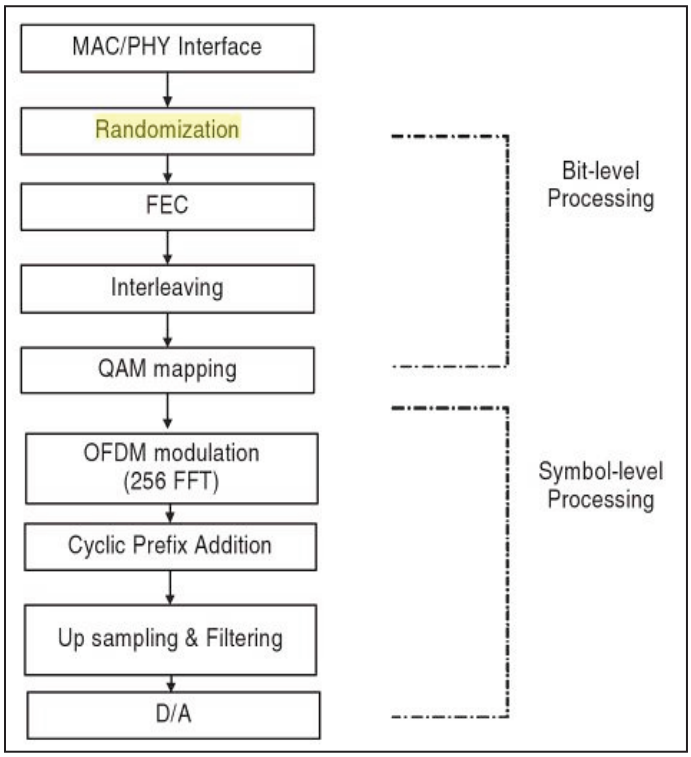

Fig. 2: Block Diagram of WiMAX Transmitter

Fig. 2 shows the transmitter system in the WiMAX system. Fig. 2 shows that there are two levels, the first level is bit-level processing and the other is symbol-level processing. At bit-level- processing, randomization is used to overcome the long sequences of "zeros" and "ones". There are XOR operations in randomization, where a Pseudo-Random Binary Sequence (PRBS) generates a random sequence which randomizes the data applying a pseudo-random sequence. Then encoding comes in the diagram, which depends upon the total slots and modulation for current transmission. The limit is set that the largest supported block, that the largest blocks cannot exceed this limit. The slots which are allocated can be concatenated to make the blocks larger of coding with the limitation not exceeding.

The next step in the transmitter part is interleaved, which is the bit level processing part of the transmitter. This is done for the protection in the transmission where long sequences have a series of errors, where these errors can be very tough to make corrections. Interleaver process is applied to the data which is the output of FEC and also encoded. The block size of interleaver depends on the bits which are coded per encoded block size. This process has two step permutation process, first part ensures that coded adjacent bits are mapped on non-adjacent bits. The second part is about the confirmation of adjacent bits are mapped on more significant bits.

Then mapper came in the system, its function is to map the data bits that are coming from interleaver and reaching to the constellation. These coded bits then mapped to the constellation and the data which is converted is also mapped to OFDM modular. This process is done in the modulation phase.

C. Receiver of Data

Then WiMAX receiver part of the system came which also has its individual block diagram. The diagram of the WiMAX receiver is given below.

There are also two processing parts of the receiver side of the WiMAX system, one is symbol level processing and the other

is bit-level processing. IFFT in the transmitter and the FFT in the receiver are performed in the modulation and demodulation of OFDM.

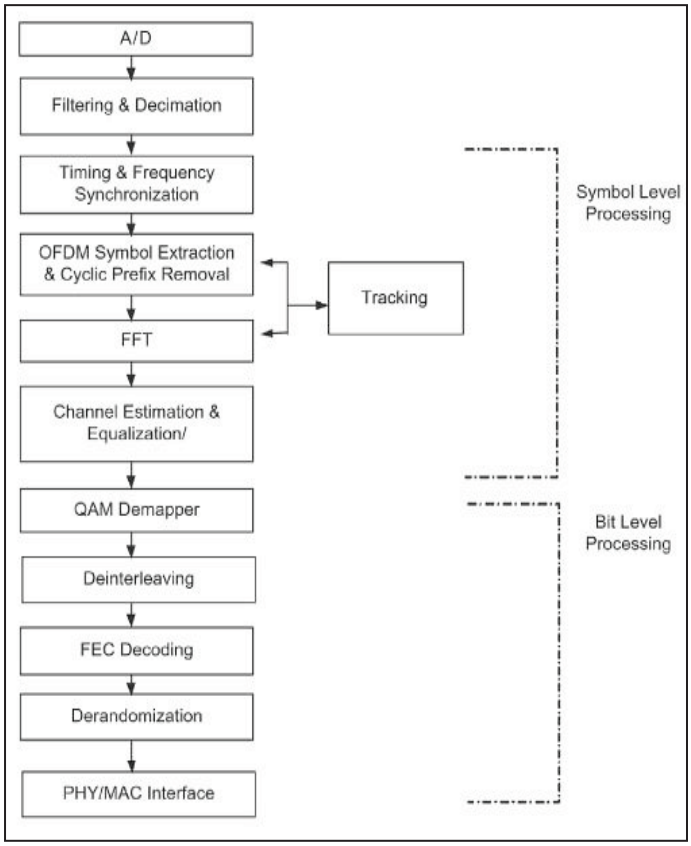

Fig. 3: Block Diagram of WiMAX Receiver.

The receiver WiMAX is the reverse process to the WiMAX transmitter process. Decoding of the data can be done at the beginning. The data which is decoded in the transmitter part firstly decoded in the receiver side. Then the de-mapper came and perform the de-mapping of the data into its original blocks. There is de-interleaving after the de-mapping and do the processing of de-interleaving of the data. In this process, the changes that are made in the interleaver level in the transmitter end are reverted and make the data into its original situation.

After the de-interleaving phase, there is a decoding phase which is the process to make the data original. The data is concatenated in the encoding phase in the transmitter side of the system and the data is reverted in this phase and the changes which are made in the encoding phase are reverted. Then the DE randomization phase came, where the changes which are made in the randomization phase are reverted. These changes may be in the form of padding added to the data. In de-randomization, these paddings are removed and make the data into its original form. Finally, the data is delivered to the receiver and to the interface.

These parts of the WiMAX system are connected using the channel. There are three most famous channel coding specified by OFDM.

1. RS-CC (Reed Solomon concatenated with convolution coding)
2. BTCs (block turbo codes)
3. CTCs (convolution turbo codes)

RS-CC is mandatory whereas BTC and CTC are optional to approach them. These channel types are supported by both uplink and downlink.

IV. Algorithm of WiMAX Model

As discussed in the previous section, the WiMAX system is divided into two parts, (i) sender (ii) receiver. Therefore the algorithm will also have two different parts first part will be about the sender side and the second part will be about the receiver side of the data. The developed algorithm is given below.

A. Sender Module

Transmit (Source)

```
1.  If  source != null
2.   R  =  randomize (source)
3.    E  =  encodeRSCC (R)
4.    InterleaveChannel (E)
5.      mapSource (Source, E)
6.       Transform_IFFT ()
7.    Else
8.   Throw exception (“transmission failed”)
```

B. Receiver Module

Receive (pack, channel)

```
1.   If  pack != null
2.        T = transform_FFT()
3.      data = De-mapSource(T)
4.       De-InterleaveChannel(data)
5.       E =  decodeRSCC (data)
6.       Data = De-randomize (e)
7.       Sink (data)
8.    Else
9.   Throw exception (“transmission failed”)
```

Above algorithm covers all the functionalities which are the part of the WiMAX model given in the previous section. The algorithm has two parts first part is the data transmitter and the second part is about the data receiver.

In the first part, firstly there is a check on the source of the data whether the data is null or not. When the source and the data is once identified, the data will be randomize, encode, interleave, mapping of data and the transform the data by different functions of the algorithm.

The second part of the algorithm receiver module and it also have the combination of the different functions. Firstly there is also a check that the data has any content or not. Then the function transformation of data came which transform the data to FFT. The data then will be de-map, de-interleave, decode the data and then de-randomize. Then finally the data will be available to the receiver.

The working of the functions in the algorithm is briefly discussed in the previous section.

V. Petri Net Model of WiMAX

Petri net is a mathematical graphical modeling language which is used for the verification of the system. As it is discussed in chapter 2 that there are many systems in which Petri nets are used for formalization purposes. So it is an easy way to make the systems formal and the nature of semi-formal of the systems can be made formal and the confusions or misunderstandings about the functionalities of the can be solved and the system may produce unique meanings to all the users and developers. In this section, a Petri net model which shows the equivalent working to the WiMAX which is shown in the figure in the previous section. Petri net is a simple graph which has a combination of places and transition and the connection between places to the transitions

can be shown by arcs. The equivalent Petri net model to fig. 4 is given below.

Fig. 4 shows the Petri net model of the WiMAX system which shows the equivalent working of the system.Petri net model also has two parts, from place p1 to p6 is transmitter part of the system and from the place, p7 to p12 is the receiver side of the system. Transition t6 is the communication channel between the transmitter and the receiver.

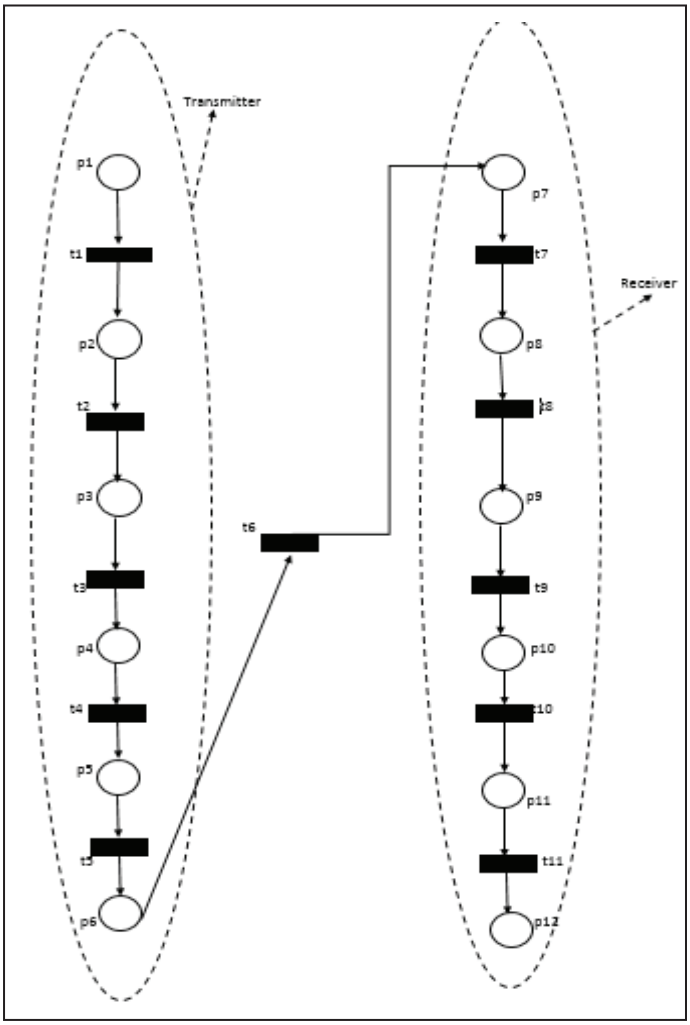

Fig. 4: WiMAX Petri Net Model.

In the PN model marked places and transitions represent the operations. In the model in figure 4, places represent the resources and operations while transitions represent the starting and ending of the operation. The detail about the transitions and places is given in below table.

Table 1 shows the functional working of WiMAX Petri net model which is developed in the previous section. In table 1 the description about all the places and transitions is given so that the users can easily understand the working of the model. "p1" is a place to identify the source and initialize the data transmitter. When the source is identified then transition "t1" is fired for the collection of the data from the transmitter.

When transition t1 is fired the model reaches at "p2" at this place, where randomization of the data is done to avoid the errors of consecutive zeros and ones. Where bits are added to the data in the randomization. Then transition "t2" is fired and concatenate the data and reaches "p3" which is the encoding phase of the data.At place "p3" encoding is enabled and transition "t3" is fired when the data is encoded using RS-CC. The model then reached "p4" which is the phase of interleaving of the data.

Table 1: Description of PN Model

S#	Places/transitions	Description	S#	Places/transitions	Description
1	p1	Source initialization	13	t1	Collection of data
2	p2	Randomize the data	14	t2	Concatenate the data for randomization
3	p3	Enable encoding	15	t3	Encode the data using RS-CC
4	p4	Proceed data for interleaver	16	t4	Done the interleaving
5	p5	Collect data to mapper	17	t5	Set the map to data
6	p6	IFFT process	18	t6	Channel
7	p7	FFT process	19	t7	Receiver initialization
8	p8	De-map the data	20	t8	Done de-mapping
9	p9	De-interleave the data	21	t9	Done de-interleaving of data
10	p10	Decoding of data	22	t10	Decode the data using RS-CC
11	p11	De-randomize phase	23	t11	Done the de-randomization and proceed to user
12	p12	Interface or sink			

When all the data is processed for interleaving the transition "t4" is fired to done the interleaving process. The model is now reached at place "p5" where data is collected for giving the map to the collected data. Then transition "t5" is fired to put maps on all the data which give the direction to the data. After the transition "t5" the model reached "p6" where IFFT process is done. IFFT process of the transmitter at the place "p6" and the FFT process of the receiver which is at the place "p7" are connected through a channel "t6". This channel "t6" is said to be the interface of communication between the transmitter of data and the receiver of the data. Then by the transition "t7" receiver is initialized and model is reached at the place "p8" which de-maps the data and decides where this data should be received. The transition "t8" is about the confirmation that the data is de-mapped successfully. The place "p9" is the process of de-interleaving of data, which means the changes applied to the data at the interleaving phase are reverted to the original position. Transition "t9" is fired when the de-interleaving of data is done to reach the place "p10" which is the decoding phase of the data. The data is encoded in the transmitter is now decoded at the place "p10". Transition "t10" is the decoding of the data using RS-CC process which is a useful technique for the decoding of data. The model then reached "p11" which is the de-randomization phase. The data is randomized in the transmitter and now de-randomize the data to its original position. Transition "t11" is done to proceed with the de-randomization of data and proceed to the interface for the user which is the place "p12". This was the whole system working about the WiMAX Petri net model which is developed and works equivalent to the block diagram of WiMAX.

VI. Verification of Petri Net Model

Most of the researchers use the reachability tree for analysis of the model constructed by Petri nets for the formalization of the system. Reachability tree is also used to check whether the system has the one-to-one functional correspondence of the model constructed by Petri nets and the original requirements of the system. This method shows all reachable places and the coverable markings of a place. The figure below shows the reachability tree of the WiMAX system where every marking of the tree shows all the places holding a token. Reachability of the model constructed by Petri net for the WiMAX system is given below.

Fig. 5 presents the verification of the WiMAX system, in which the markings have the places which have the tokens at the same time.And all the reachable places from the current place.

Mi	Marking	Description
M1	P1	Source identification
M2	P2	Randomizer
M3	P3	RS-CC Encoder
M4	P4	Channel interleaver
M5	P5	Mapper
M6	P6	IFFT
M7	P7	FFT
M8	P8	De-Mapper
M9	P9	Channel De-interleaver
M10	P10	RS-CC Decoder
M11	P11	De-Randomizer
M12	P12	Sink (interface)

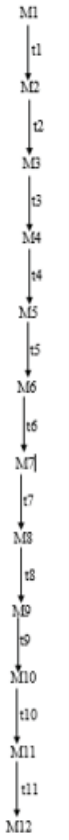

Fig. 5: Verification of Petri Net model.

The table shows that all the places have one-to-one functional correspondence and there is no repetition in the reachability tree. This results that the system is formally verified. The system is at the final place when all the transitions have been fired.

VII. Conclusion

In this study, we developed a Petri nets model of WiMAX system which is semi-formal and there can be chances of threats and data transmission errors. At the beginning of this work, we analysed that the WiMAX protocol is semi-formal and can have errors and threats. Then the block diagram of the WiMAX protocol is developed first and it is translated into a Petri net model which covers all the functionalities of the WiMAX system. There is an algorithm about the WiMAX protocol is developed which also covers the system's working. Finally, the verification of the Petri net model is done by reachability tree. Hence, the WiMAX protocol is formally verified and the chances of errors and data loss in the protocol are minimized.

References

[1] Agarwal, A., Mehta, S. N.,"Combined Effect of Block interleaving and FEC on BER Performance of OFDM based WiMAX (IEEE 802.16 d) System", American Journal of Electrical and Electronic Engineering, 3(1), 4-12, 2015.

[2] Agarwal, B.,"Transformation of UML Activity diagrams into Petri nets for verification purposes", International Journal of Engineering and Computer Science, 2(03), 2013.

[3] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.,"Internet of things: A survey on enabling technologies, protocols, and applications", IEEE Communications Surveys & Tutorials, 17(4), pp. 2347-2376, 2015.

[4] Alhroob, A., Dahal, K., Hossain, A.,"Transforming UML sequence diagram to high-level Petri Net. In Software Technology and Engineering (ICSTE), 2nd International Conference on (Vol. 1, pp. V1, 2010.

[5] Andrews, J. G., Claussen, H., Dohler, M., Rangan, S., Reed, M. C.,"Femtocells: Past, present and future", IEEE Journal on Selected Areas in communications, 30(3), pp. 497-508, 2012.

[6] Centenaro, M., Vangelista, L., Zanella, A., Zorzi, M., "Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios", IEEE Wireless Communications, 23(5), pp. 60-67, 2016.

[7] Chung, J. M., Park, K., Won, T., Oh, W., Choi, S.,"New protocols for future wireless systems", In Circuits and Systems (MWSCAS), 2010 53rd IEEE International Midwest Symposium on (pp. 692-695). IEEE, 2010.

[8] Henda, N. B., Norrman, K.,"Formal analysis of security procedures in LTE-A feasibility study", In International Workshop on Recent Advances in Intrusion Detection (pp. 341-361). Springer, Cham, 2014.

[9] Hsiang, H. C., Shih, W. K.,"Improvement of the secure dynamic ID-based remote user authentication scheme for a multi-server environment. Computer Standards & Interfaces, 31(6), 1118-1123, 2009.

[10] Iqbal, R. S., Ahmad, S., Khan, S. A.,"A Mobile-Agent Environment for Service Oriented System using Strong Mobility. VFAST Transactions on Software Engineering, 8(1), pp. 10-18, 2015.

[11] Iv, R. G. P., Gomaa, H.,"Validation of dynamic behavior in UML using Colored Petri nets", In Proc. of UMLt'2000 Workshop-Dynamic Behavior in UML Models: Semantic Questions, Vol. 1939, pp. 295-302, 2000

[12] Jensen, K., Kristensen, L. M., Wells, L.,"Coloured Petri Nets and CPN Tools for modeling and validation of concurrent systems", International Journal on Software Tools for Technology Transfer, 9(3-4), pp. 213-254, 2007.

[13] Khan, S. A., Iqbal, R. S., Zafar, N. A., Ahmad, F.,"Flood Analysis and Prediction Support based on UML and Mobile Petri Net Specification and Verification", In Proceedings of the World Congress on Engineering and Computer Science (Vol. 1), 2012.

[14] Komninos, N., Philippou, E., Pitsillides, A.,"A survey in the smart grid and smart home security: Issues, challenges, and countermeasures", IEEE Communications Surveys & Tutorials, 16(4), pp. 1933-1954, 2014.

[15] Narayana, P., Chen, R., Zhao, Y., Chen, Y., Fu, Z., Zhou, H.,"Automatic vulnerability checking of IEEE 802.16 WiMAX protocols through TLA+," In 2006 2nd IEEE Workshop on Secure Network Protocols (pp. 44-49). IEEE,

2006.
[16] Odell, J.,"Advanced Object-Oriented Analysis and Design Using UML". SIGS Reference Library. Cambridge (1998) 0-521-64819-X.
[17] Prakash, G., Pal, S.,"WiMAX technology and its applications", International Journal of Engineering Research and Applications, 1(2), pp. 327-336, 2012.
[18] Raychaudhuri, D., Mandayam, N. B.,"Frontiers of wireless and mobile communications", Proceedings of the IEEE, 100(4), pp. 824-840, 2012.
[19] Shaddad, R. Q., Mohammad, A. B., Al-Gailani, S. A., Al-Hetar, A. M., Elmagzoub, M. A.,"A survey on access technologies for broadband optical and wireless networks", Journal of Network and Computer Applications, 41, pp. 459-472, 2014.
[20] Staines, T. S.,"Transforming UML sequence diagrams into Petri Net", Journal of communication and computer, 10(1), pp. 72-81, 2013.
[21] Wang, C., Chow, S. S., Wang, Q., Ren, K., Lou, W., "Privacy-preserving public auditing for secure cloud storage", IEEE Transactions on Computers, 62(2), pp. 362-375, 2013.
[22] Zhang, L., Estrin, D., Burke, J., Jacobson, V., Thornton, J. D., Smetters, D. K., Papadopoulos, C.,"Named data networking (NDN) project", Relatório Técnico NDN-0001, Xerox Palo Alto Research Center-PARC, 157-158, 2010.
[23] Zhao, Y., Fan, Y., Bai, X., Wang, Y., Cai, H., Ding, W.,"Towards formal verification of UML diagrams based on graph transformation", In E-Commerce Technology for Dynamic E-Business, IEEE International Conference on, pp. 180-187. IEEE, 2004.