EAP - Based Load Minimization for Fast and Secure Inter ASN Handovers in Mobile WiMAX Networks

Group Members:
Anton John Karthik.J
Santhosh Kumar.R
Shyam Mohan.K

Guided by:
Prof.S.J.K.Jagadeesh Kumar

Department of Computer Science and Engineering
Sri Krishna College of Technology

DETAILS OF BASE PAPER

- Title : Enhanced EAP-Based Pre-Authentication for Fast and Secure Inter-ASN Handovers in Mobile WiMAX Networks
- Journal : IEEE Transactions on Wireless Communications
- Volume : Volume 11, No.6,
- Dated : June 2012.
- Authors : Thuy Ngoc Nguyen
  Dr. Maode Ma

ABSTRACT

- Mobile WiMAX networks have already met the expectations of mobile users in providing secured and seamless service.
- The time consuming authentication procedure which causes service disruptions was solved using the EAP (Extensible Authentication Protocol) scheme. But the problems of overloading and flooding of data in the ASNs still exist.
- The proposed system involves identifying border base stations and differentiating them from the interior base stations. According to this method, only the border base stations are allowed to transfer the control information related to a MS to the neighboring ASNs.
- Since the interior base stations are prevented from sending any packets to the tASN, the load on the tASN is considerably reduced. It prevents flooding of data at the tASN, thereby enhancing the efficiency and the performance of ASNs.

INTRODUCTION

- **WiMAX** (**Worldwide Interoperability for Microwave Access**) systems were designed at the outset with robust security and speedy access in mind. The methods for reducing time delay and ensuring data privacy were achieved through EAP handover technique.
- However, users will not be satisfied when the system slows down, because of overload and data traffic.
- Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests.

….cont.

- A Handover is the process of transferring an ongoing call or data session from one channel connected to the core network to another.
- The WiMAX technology specifies a variety of handover schemes to the transfer of call or data from the control of one network to another.
- The load on the WiMAX systems is nothing but the data that is transferred from one node to another and the control information that facilitates the transfer of data.

LITERATURE SURVEY

Reference Paper 1

- Title: Inter-ASN Handover using MSCTP Protocol in IEEE 802.16e Networks
- Year: 2009
- Journal: Seventh Annual Communication Networks and Services Research Conference
- Authors: Tarek Bchini
  Nabil Tabbane
  Sami Tabbane

....cont.

- MSCTP is based on multi-homing, which allows a MS to have multiple IP addresses among which one address is chosen as the primary address and is used as the destination address for normal transmission.
- When an MS moves to a foreign network, it receives an IP address from the foreign network by DHCP. The MS is now able to establish a communication with the DS using this secondary address.

Drawbacks:

- Time Consuming
- Security Breaches like Man-in-the-Middle, Replay and DOS

….cont.

Reference Paper 2

- Title: A Simplified ASN Anchored Mobility Scheme over Mobile WiMAX
- Year: 2009
- Journal: First Asian Himalayas International Conference
- Authors: Shaoh-Chen Ke
  I-Husan Peng

….cont.

- This method focuses on improving the performance of the mobility by the usage of simplified ASN anchored mobility scheme.
- The scheme modifies the handover procedure by including an additional ASN named anchor ASN and uses encapsulation technique thereby obtaining inter ASN handover with reduced latency.
- The security is also strengthened as only the anchor ASN maintains all the key contacts

Drawback:

- Co-ordination between the functions of the ASN equipments is still an issue.

….cont.

Reference Paper 3

- Title: Extensible Authentication Protocols for IEEE standards 802.11 and 802.16
- Year: 2008
- Journal: Fifth International Conference on Mobile Technology, Applications, and Systems
- Authors: D.Q.Liu
  M.Coslow

….cont.

- EAP-based authentication uses a backend authentication server(AS), which allows users to choose an authentication method suitable for the existing credentials without requiring the authenticator to be updated to support each new authentication approach.
- When a MS undergoes an inter-ASN handover, it performs a full EAP authentication with the AS and performs a 3-way handshake with the BS to distribute the Traffic Encryption Key (TEK).

Drawbacks:

- Costly due to its time consuming public key cryptography operations
- Delay of several round trips between the MS and the AS
- A full EAP authentication takes 1000ms, while recommended minimum handover latency is 150ms.

....cont.

Reference paper 4

- Title: Extensible Authentication Protocol(EAP) Early Authentication Problem Statement
- Year: 2010
- Journal: International Symposium on a World of Wireless Mobile and Multimedia Networks
- Authors: Y. Ohba
  G. Zorn

….cont.

- The protocol proposed here, called as Handover Early Authentication Protocol(HOEA), utilizes pro-active signalling to discover candidate access network, where the MS potentially moves to and performs a full EAP authentication before it attaches to the candidate network.

Drawbacks:

- It only works when the link layer supports pro-active signalling
- A possibility that the handover has already started before the completion of the pre-authentication phase, resulting in a failed pre-authentication
- Wastage of unnecessary effort in key exchange between the MS and the neighbouring ASNs

…cont.

Reference Paper 5

- Title: Enhanced EAP-Based Pre-Authentication for Fast and Secure Inter-ASN Handovers in Mobile WiMAX Networks
- Year: 2012
- Journal: IEEE Transactions on Wireless Communications
- Authors: Thuy Ngoc Nguyen
  Dr. Maode Ma

....cont.

- In order to enhance the security functionality and the efficiency of the EPA, a new technique called, EAP-Transport Layer Security(EAP-TLS) based pre-authentication(EEP) scheme which can prevent Denial of Service and Replay Attacks with much less computational and communication resources and at the same time, can overcome the drawbacks of the previous methods.

Drawbacks:

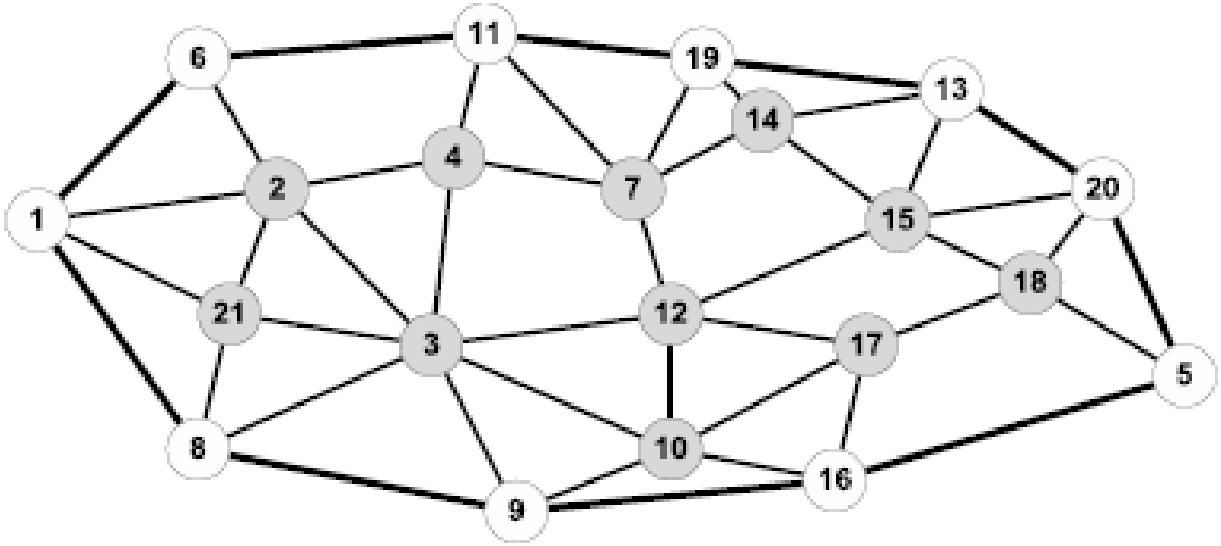
- Overloading of ASN
- Data traffic may result in slowing down of the network

PROBLEM STATEMENT

- In EAP – based scheme, whenever a MS registers itself to the hASN, the related control information is transmitted to all its neighboring ASNs. Since, all these control information may not be used in near future, the load on the tASN is considerably increased, leading to problems like overloading and flooding of data. Hence, the base stations at a fixed minimum distance from the border are classified as Border Base Stations (bBS), using Localized Algorithm for Border Node Detection. As the control information is transmitted to the tASN, only from these bBS, the load on the tASN is reduced and its performance is enhanced.

PROPOSED WORK

- In order to reduce the overloading of the target ASN(tASN), we propose the EAP - Based Load Minimization Technique.
- In this technique, we differentiate the border base stations from the interior base stations, as shown in the figure below.



...cont.

- By this method, only when the MS enters the range of the border base stations, the hASN sends the control information to the tASN, thereby limiting the number of base stations involved in the process.
- It reduces the number of pre-authentication request messages from the hASN to the tASN.
- The technique provides a fast and secured inter-ASN handover with reduction in the load on the tASN and thereby enhances the performance of the tASN.

MODULES

- **Module 1: Simulation of Handovers in WiMAX**

The simulation involves both the intra-ASN and inter-ASN handovers depicting the movement of the MS between the control of one BS to another within the same and different ASN's respectively.

- **Module 2: Implementation of Extensible Authentication Protocol**

We simulate the EAP which shows the transfer of control information between the two ASN's using the Pair-Wise Master Key (PMK) generated using a hash function.

- **Module 3: Implementation of Load Minimization Scheme**

The load on the ASN is minimized, by the selective transfer of control information in the inter-ASN handovers, leaving out the unnecessary ones.

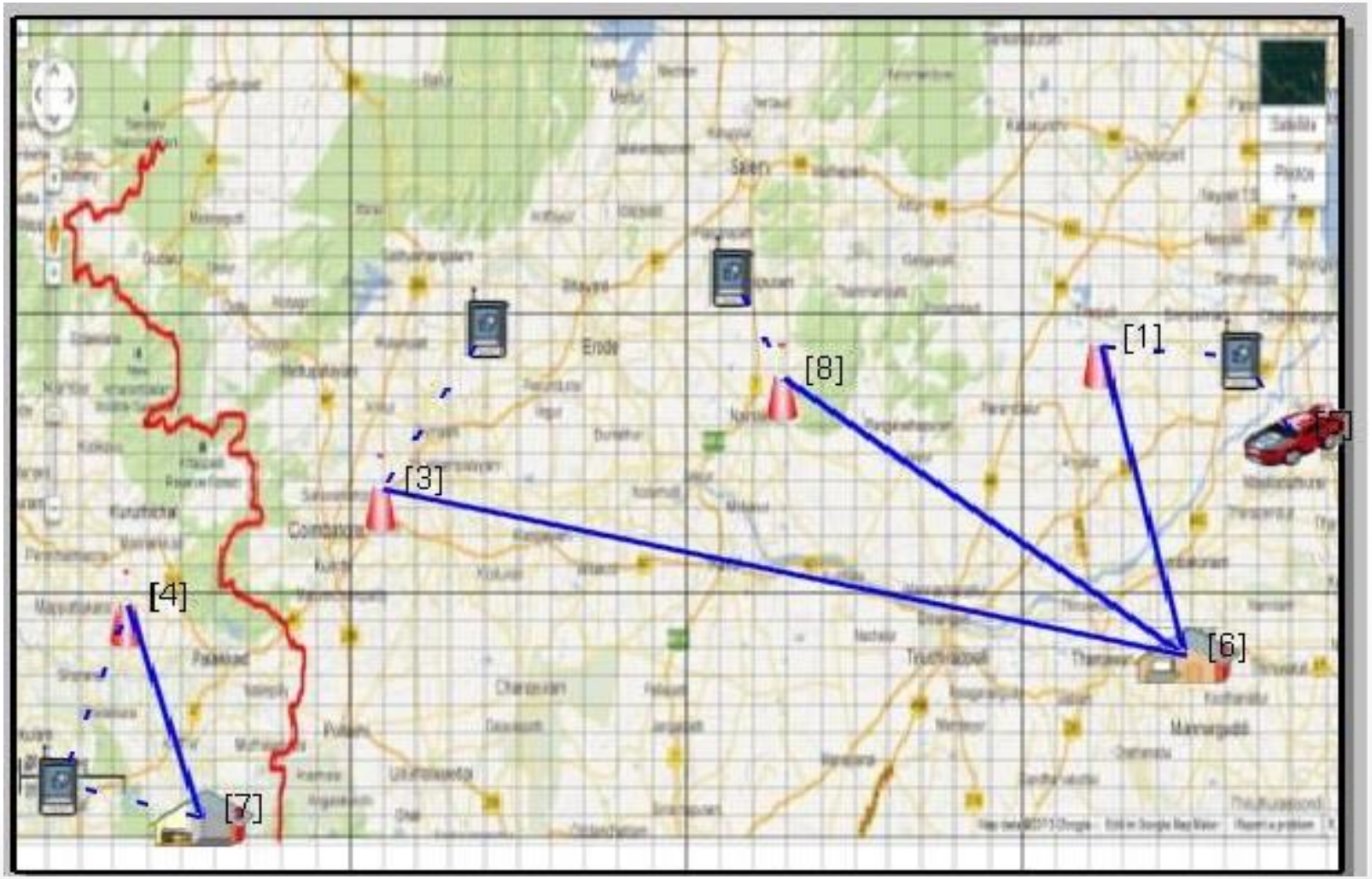
Simulation of Handovers in WiMAX

- For simulating a WiMAX handover, the components required are Mobile Stations (MS), Base Stations (BS), Home Base Stations (hBS), Target Base Stations (tBS), Home Access Service Network (hASN) and Target Access Service Network (tASN).
- At first, the MS registers itself to any BS within the range of a particular ASN, called hASN.
- When the MS moves within the range of the hASN, the control is transferred from one BS to the next, called as intra-ASN handover.
- But when the MS moves from the BS of one ASN to the BS under the control of another ASN, called tASN, it results in an inter-ASN handover.

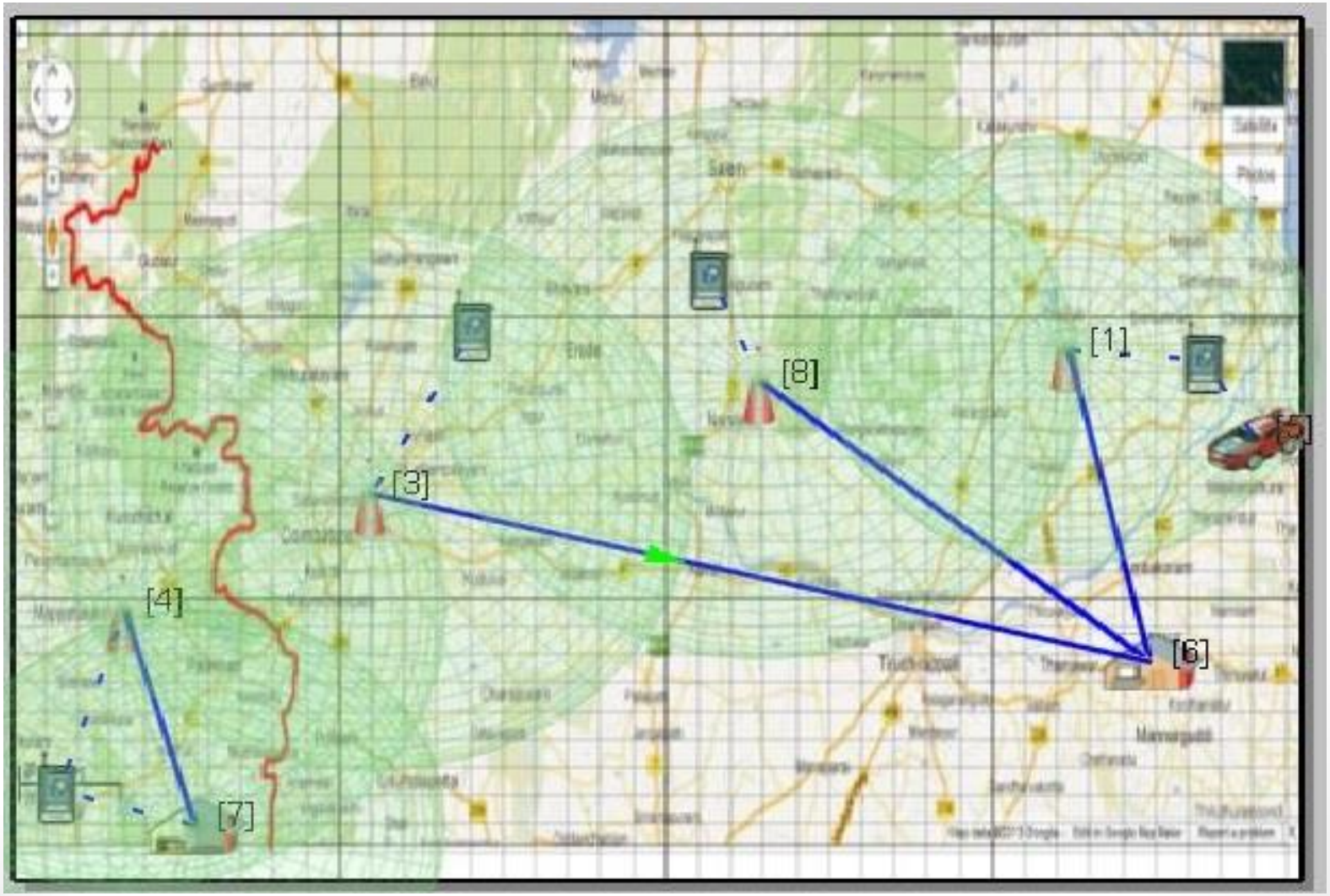
Attribute	Value
Radio Type	802.16 Radio
Transmission Power	20.0
Routing Protocol	Bellman Ford
Antenna Gain(dB)	12.0
Antenna Height(Mtr)	10
Antenna Efficiency(dB)	0.8
Antenna Model	Omni directional
Temperature(k)	290.0
Noise Factor(dB)	10.0
Packet Reception Model	PHY 802.16 Reception Model

Parameters Required for Simulation

SCREENSHOT 1



SCREENSHOT 2



Implementation of EAP

- In EAP, whenever the MS registers itself to any BS within the range of the hASN, the identities are fetched by the respective BS and are sent to the hASN.
- The hASN receives the identities and shares the Message Authentication Code (MAC) key with the MS. The MS sends an acknowledgement message back to the hASN. The entire process is termed as EAP-TLS based three-way handshake.
- After this, the hASN sends the PRE_Auth_Init packet which contains the 16-bit Session Identifier (SId), Neighbor List (NBL) and the MAC key to the MS.

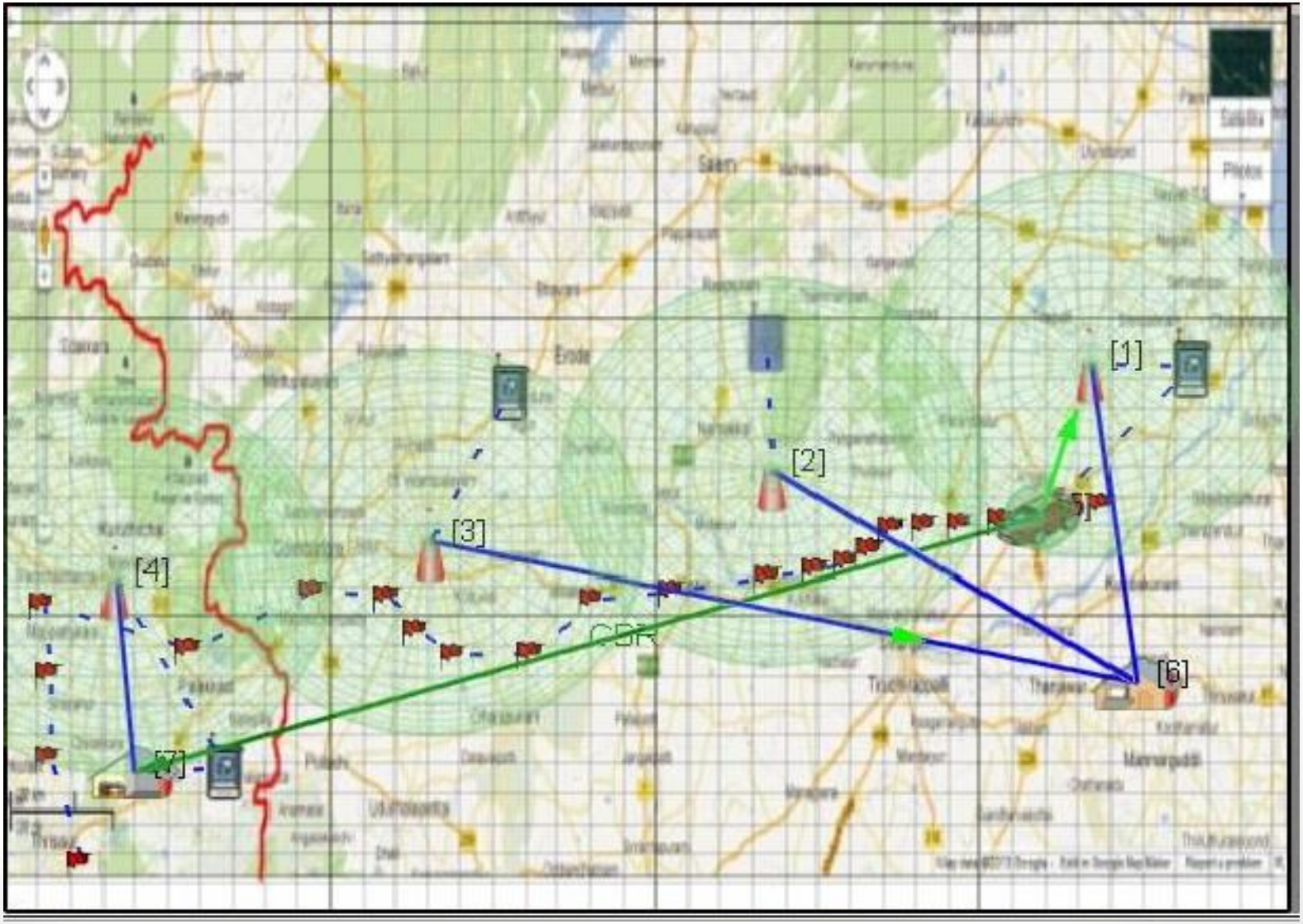
…cont.

- The MS checks for the integrity of the message and then generates a pseudo-random number, X_i called Pre-Master Secret (PMS). It then sends Sid and Id of the MS along with the PMS to the hASN.
- On receiving the packet, the hASN relays it to all the tASNs. The tASN verifies the integrity of the message and then decrypts it to obtain the PMS.
- For the PMS X_i , the tASN generates the pseudo-random number Y_i , which is sent to the MS via the hASN. The pseudo-random numbers X_i and Y_i are used to generate the Master Secret Key (MSK) at both ends.

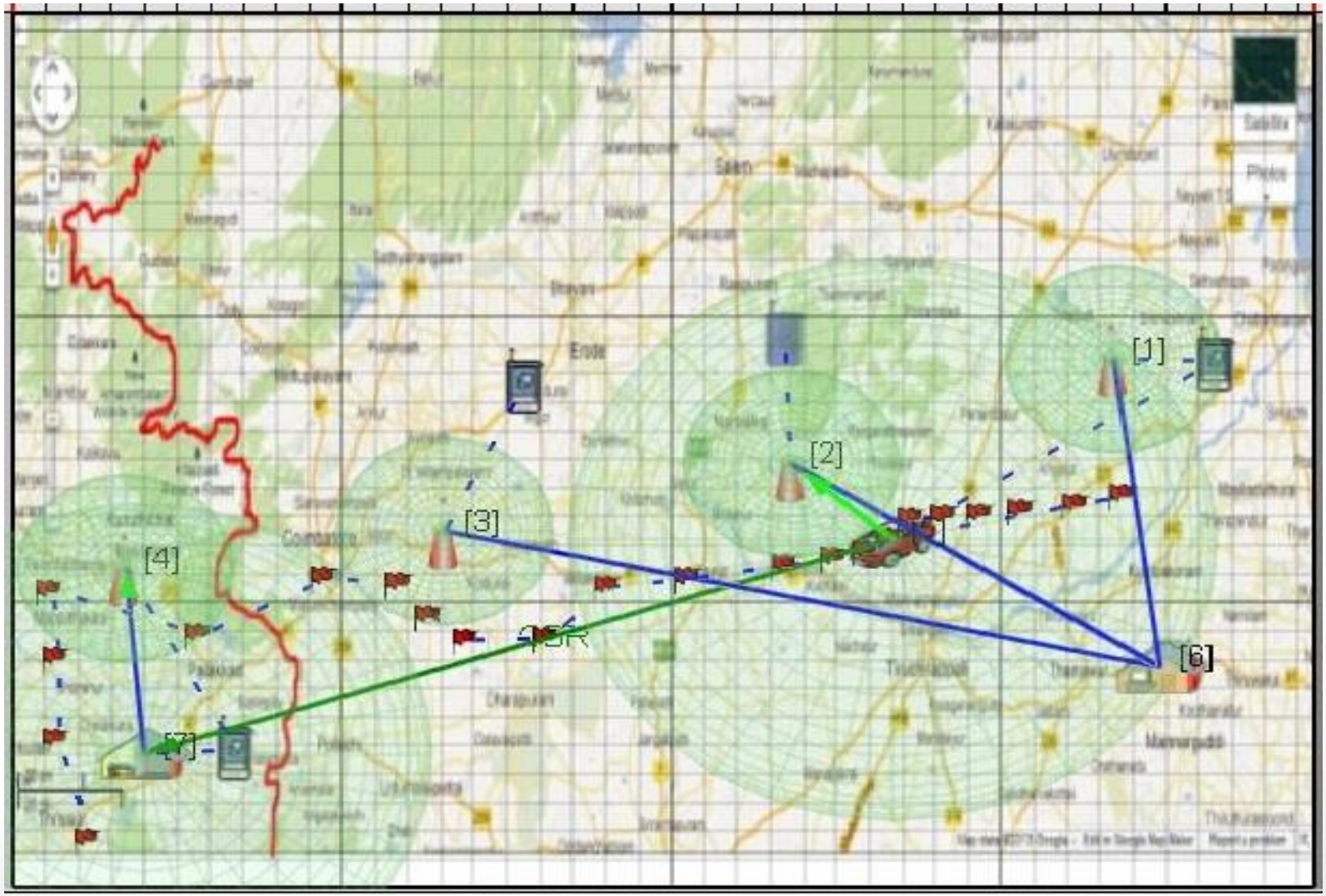
…cont.

- When the MS enters the range of the tASN after the inter-ASN handover, the MSK is sent to the tASN. The tASN receives the MSK and verifies it, thereby authenticating the MS. This phase is called the re-authentication.

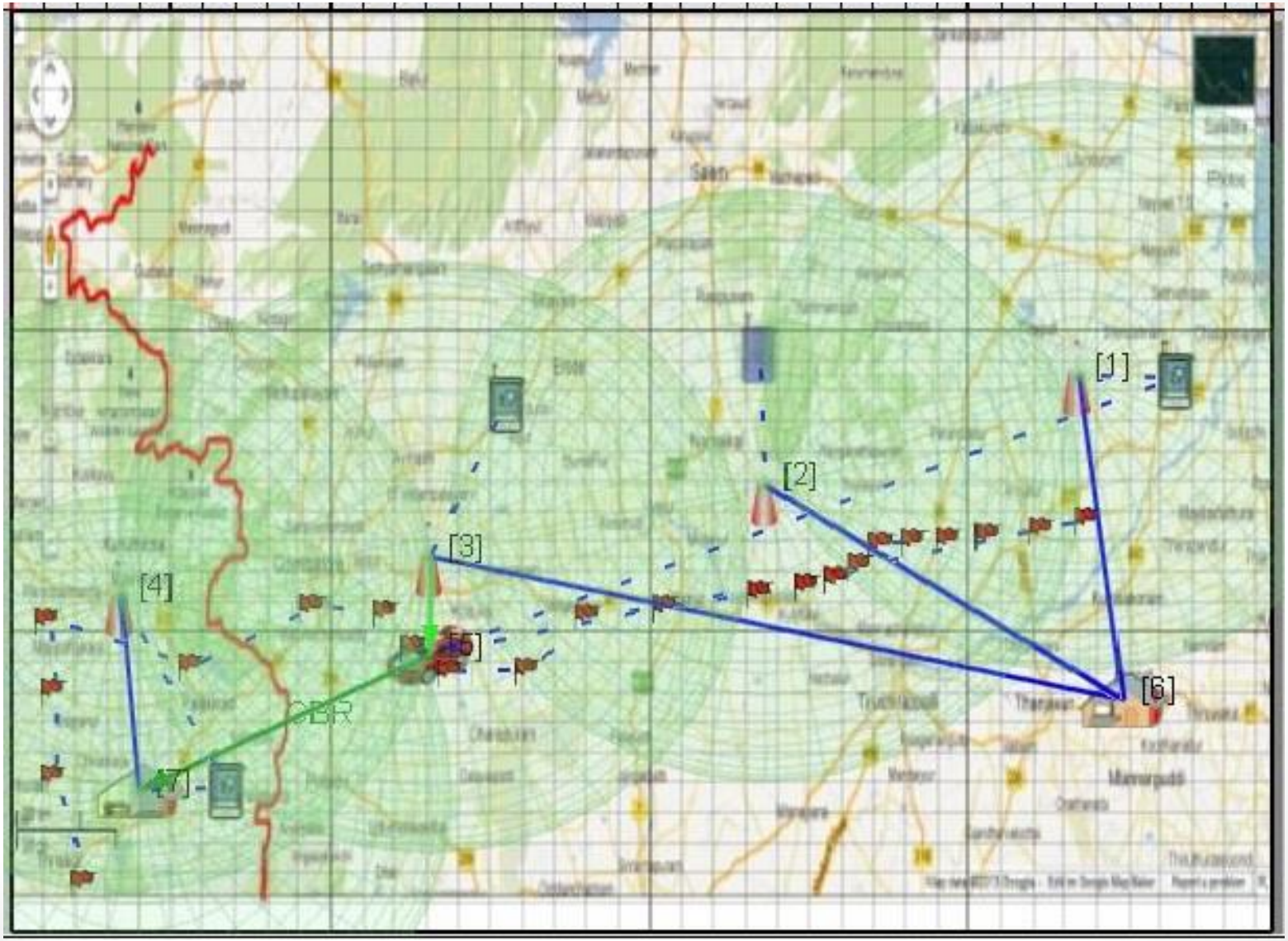
SCREENSHOT 1



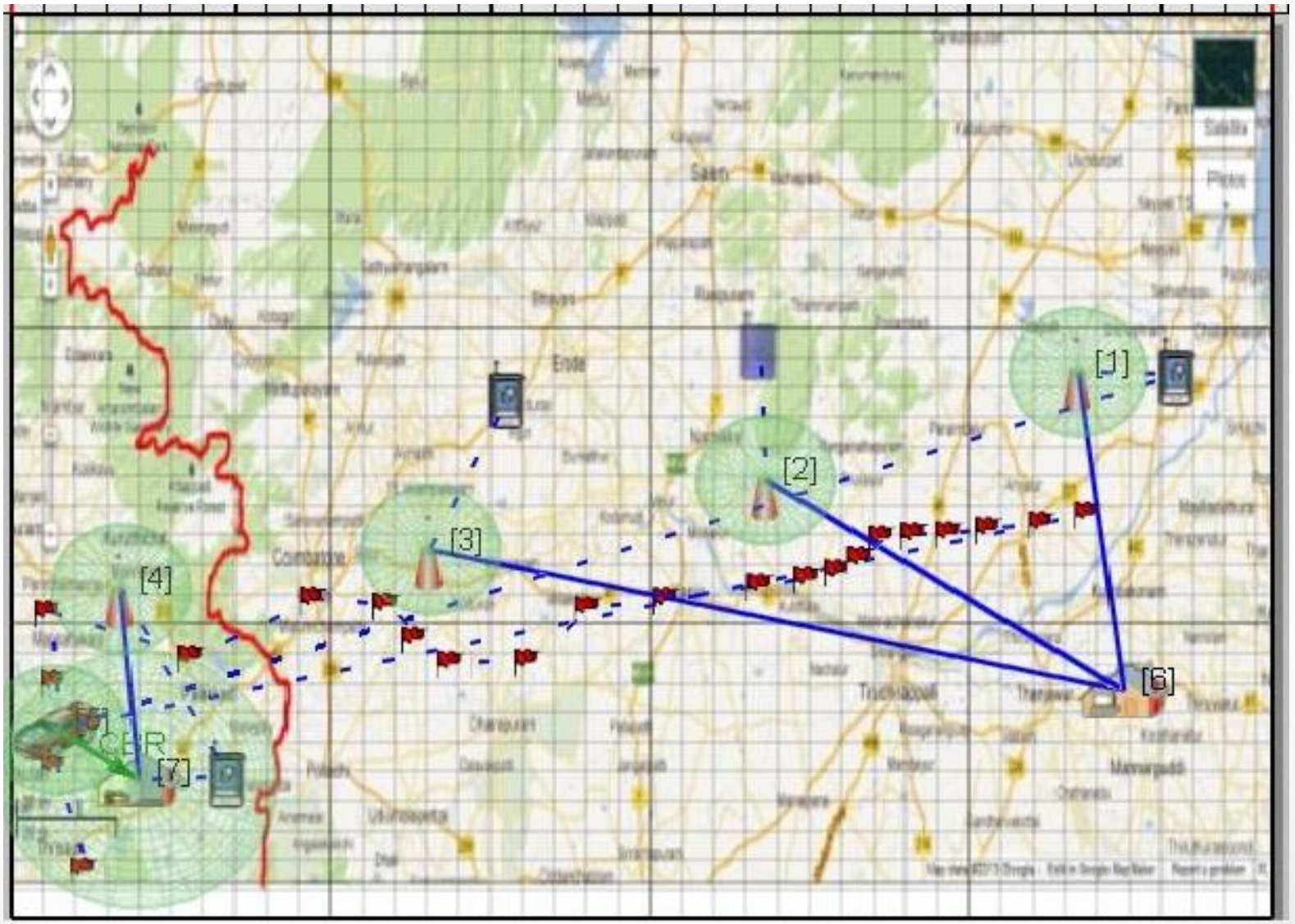
SCREENSHOT 2



SCREENSHOT 3



SCREENSHOT 4



Implementation of EAP-based Load Minimization

- The proposed method focuses on identifying the base stations which form the boundary of the ASN called as Border Base Stations (bBS). The rest of the base stations are classified as Interior Base Stations (iBS).
- This method uses a Localized Algorithm for Border Node Detection. In this algorithm, we consider a network topology N.
- To classify a node as a border node B, it has to satisfy the following properties:
    1. B is a connected sub-graph of the graph N
    2. The connected nodes in B should form the boundary for the area, that bounds all the other interior nodes.

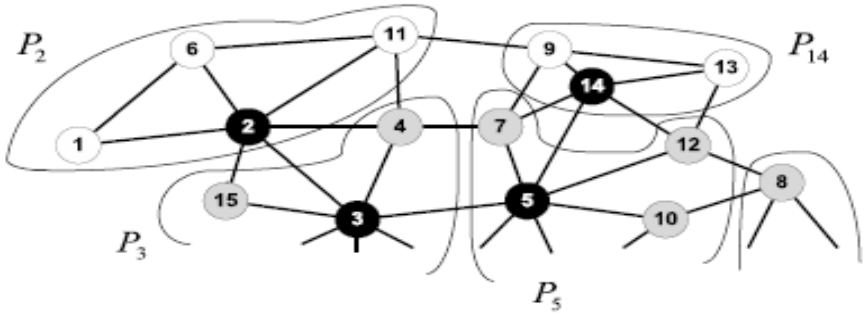
…cont.

- The topology N is divided into smaller segments called **packs**, which contains a centre node called Head and subset of its adjacent nodes called descendants. If n_i is the head of the pack, then the pack is denoted by P_i .
- It is assumed that every n_i in the network is able to obtain the number of its neighbors (d_i).
- Using d_i, we derive a new parameter called relative connectivity (r_i) using the following formula.

$$r_i = d_i - \frac{1}{d_i} \sum_{n_j | a_{ij}=1} d_j .$$

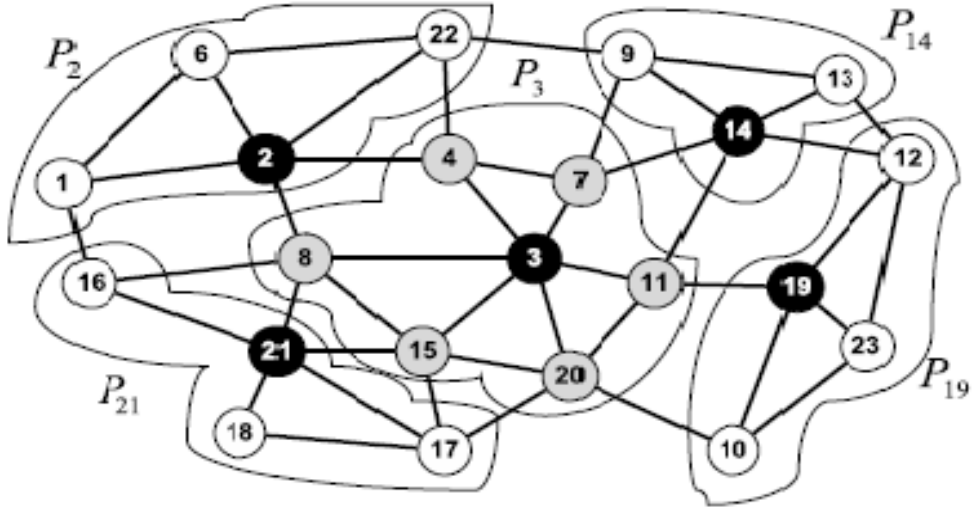
…cont.

- r_i defines the difference between the connectivity of n_i and its neighbors. If $r_i > 0$, it indicates that n_i's connectivity is above the average connectivity within its neighborhood. If $r_i < 0$, it indicates poor connectivity.
- r_i is used for pack construction. The packs are constructed by merging the nodes with the best connected neighbors. A node n_i which is not adjacent to a less connected node is not included in the pack.
- The best connected node becomes the head of the pack and the rest become the descendants.



…cont.

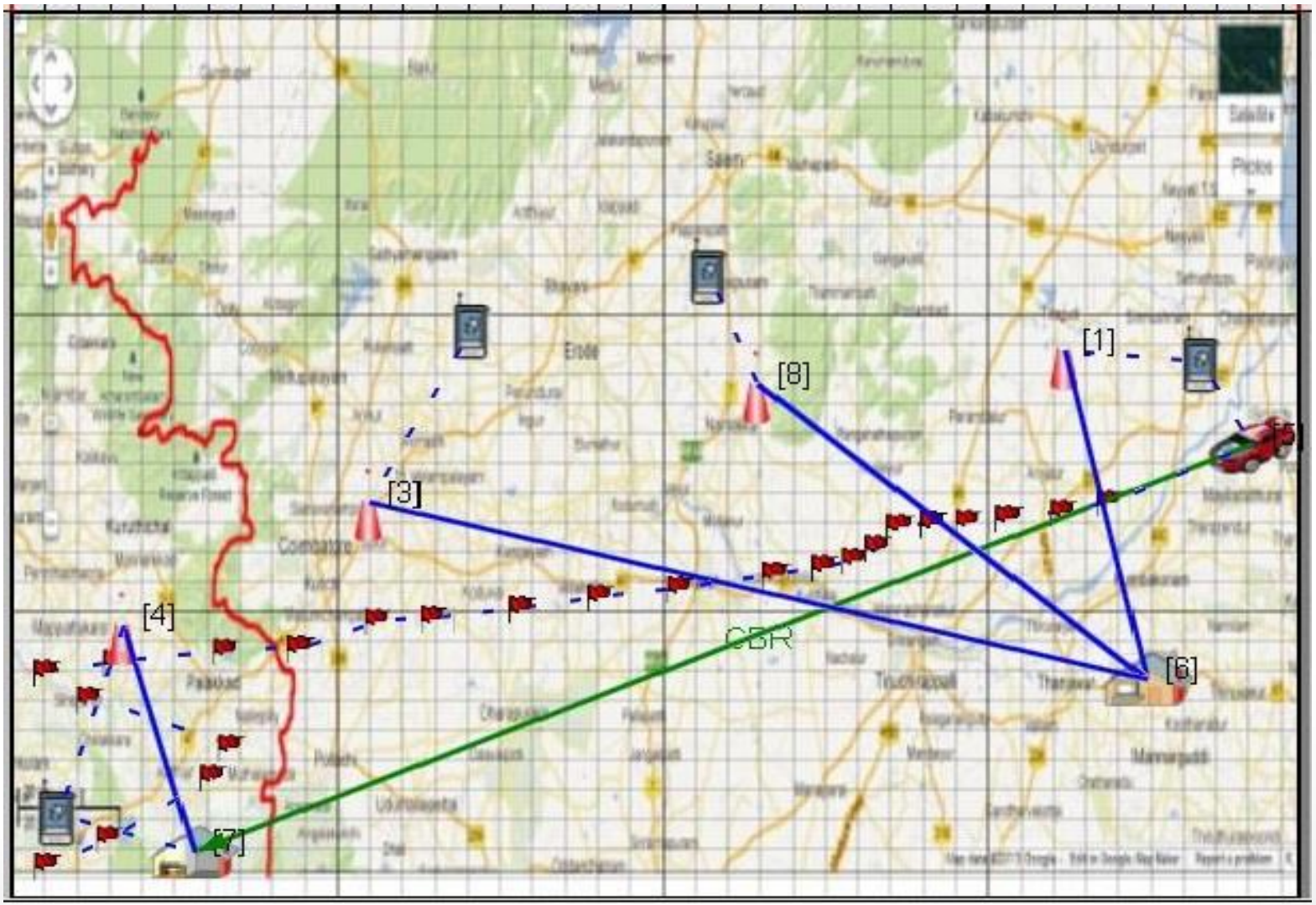
- If a node is already the descendant in another pack, it selects the better connected head. Thus, two types of packs are formed:
    1. Packs consisting of the border nodes
    2. Packs containing no border nodes



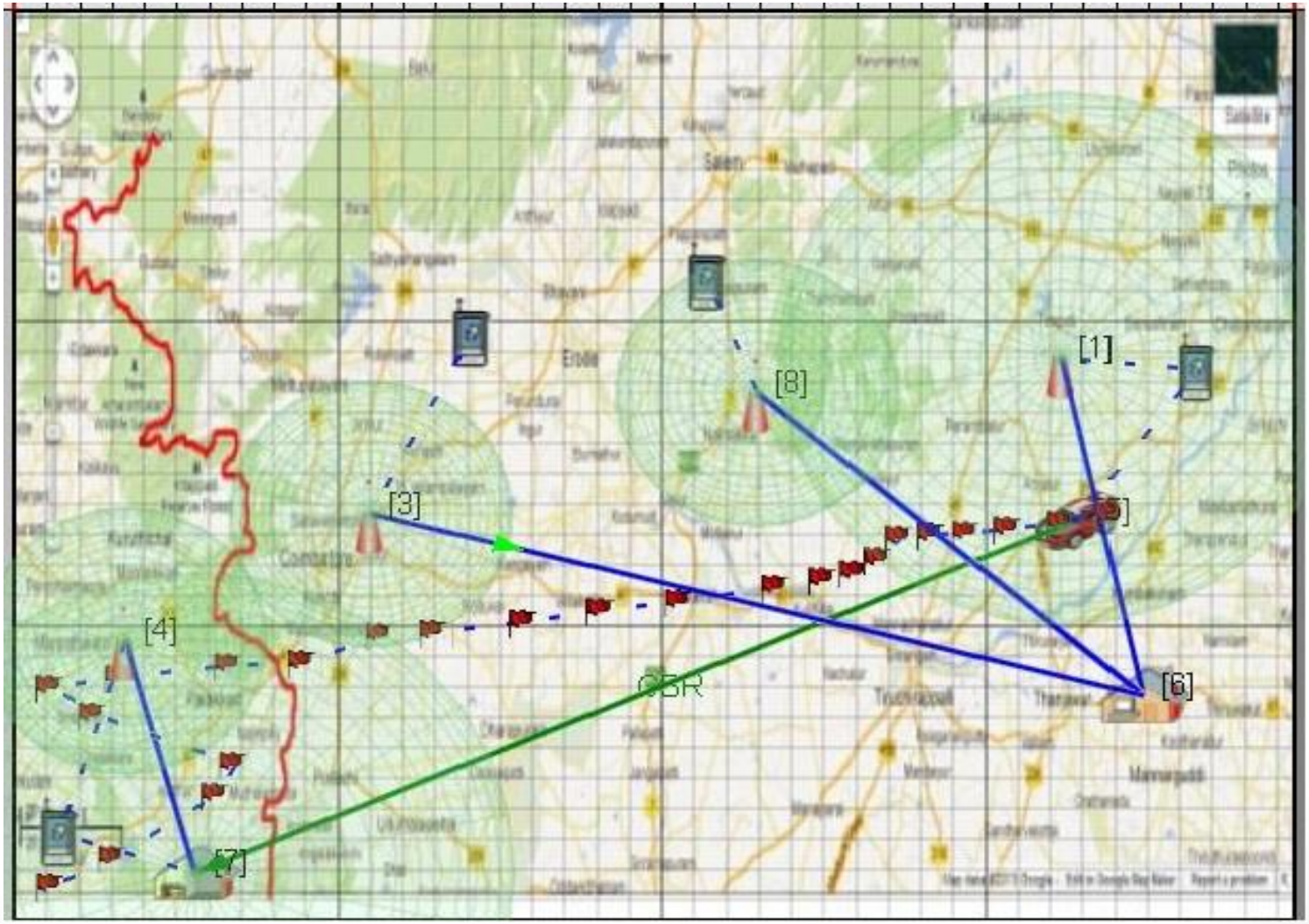
…cont.

- The packs with border nodes are considered. All the descendants of that pack are classified as border nodes.
- According to this scheme, the MS can register itself to any BS under the hASN. But, the pre-authentication phase is initiated only when the MS enters the range of the bBS.
- By this method, only when the MS reaches the range of the bBS, the hASN sends the control information to the tASN, thereby limiting the number of base stations involved in the process.
- As the iBS are not allowed to send any data to the tASNs, the load on the ASN will be considerably reduced.

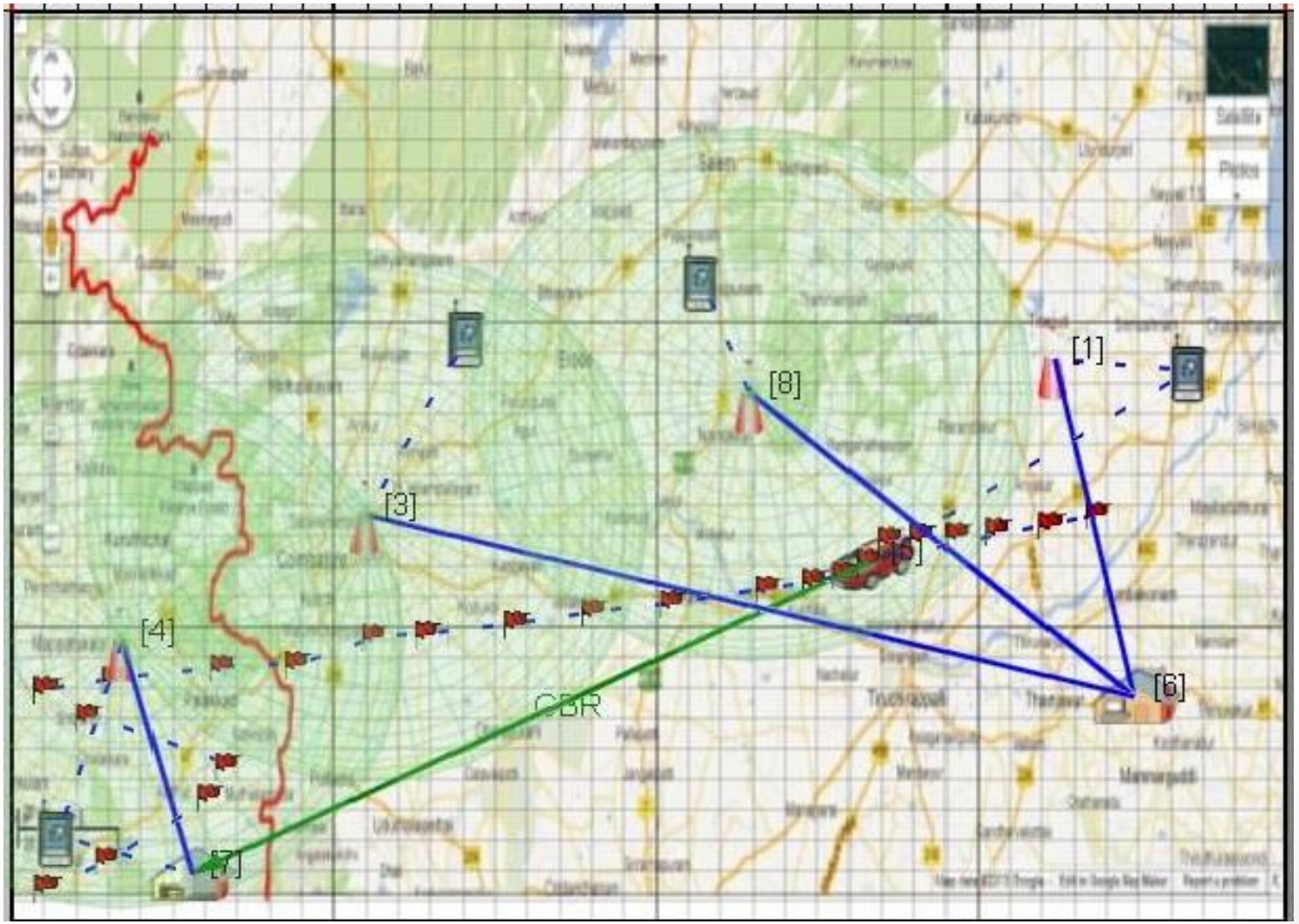
SCREENSHOT 1



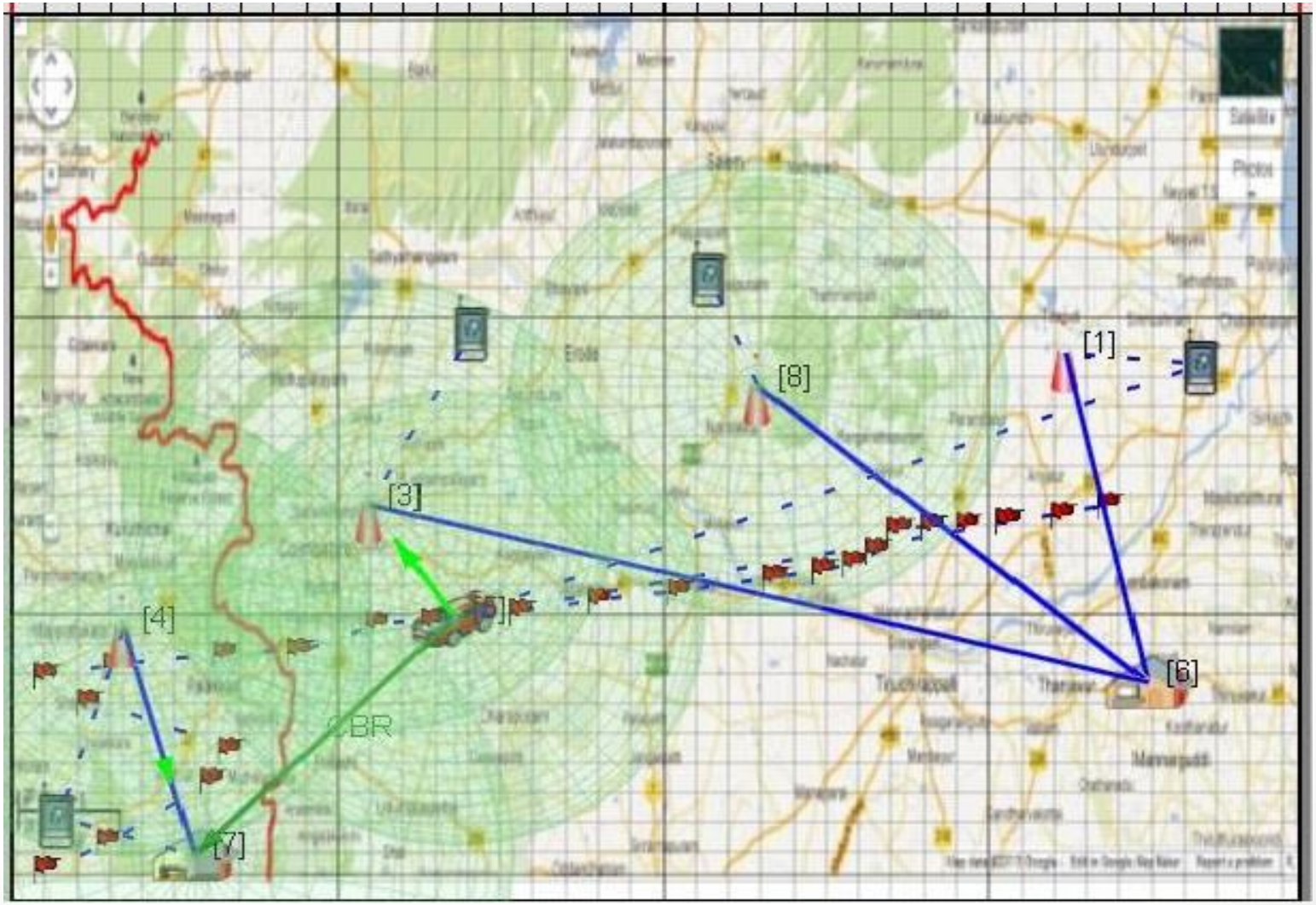
SCREENSHOT 2



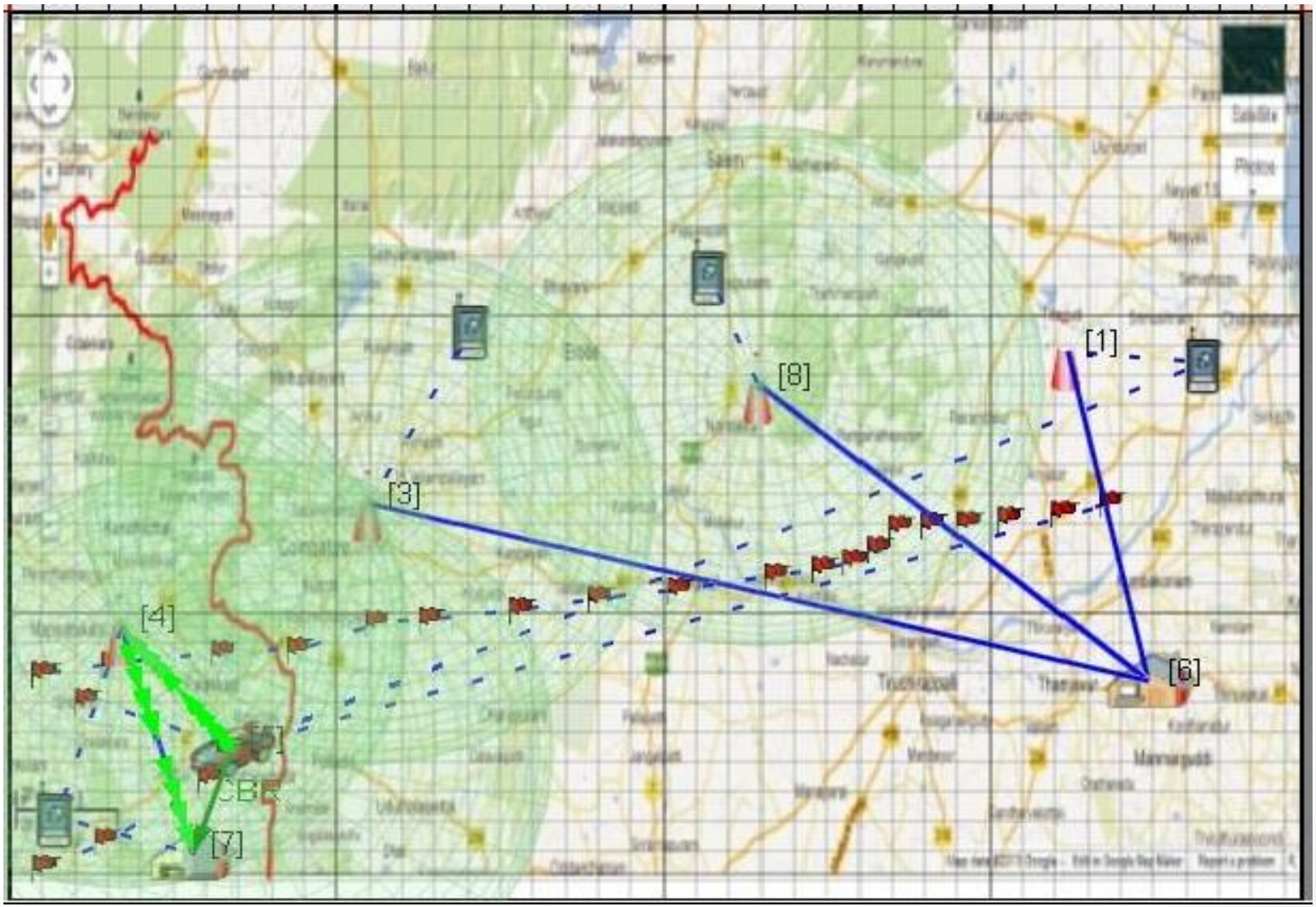
SCREENSHOT 3



SCREENSHOT 4

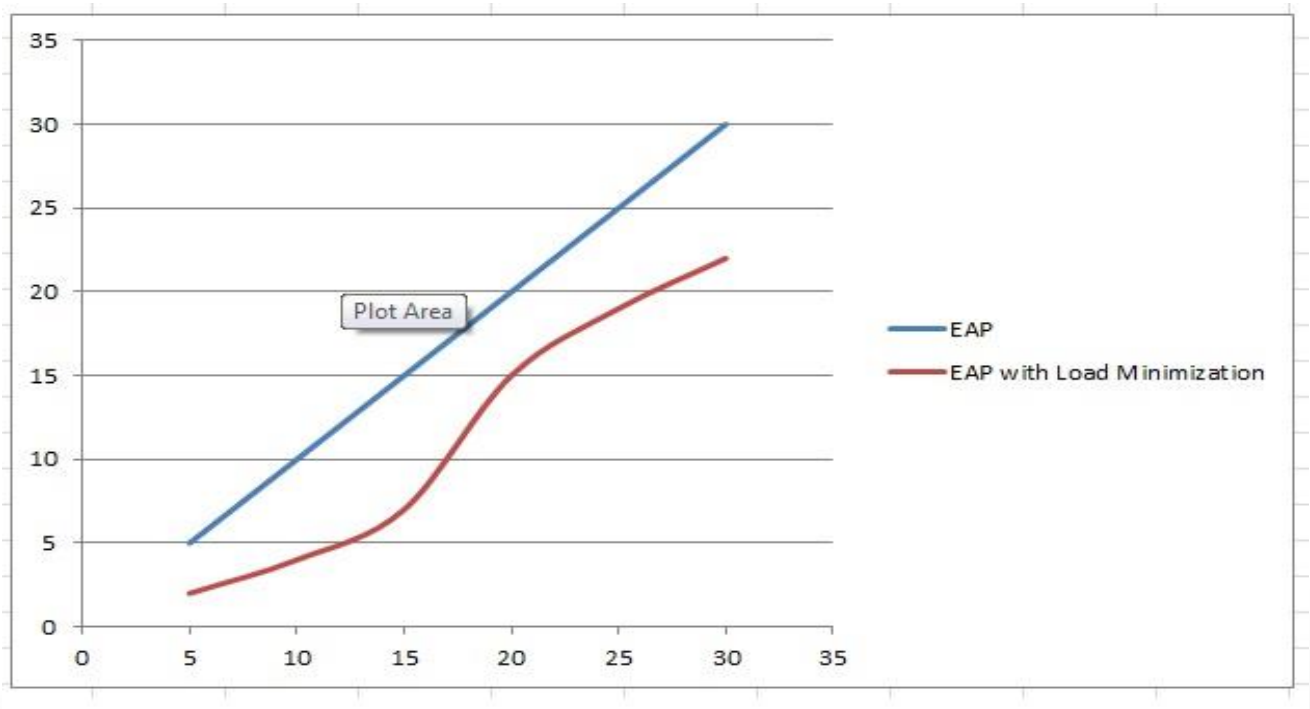


SCREENSHOT 5



PERFORMANCE ANALYSIS

- The graph shown below depicts a comparison between the existing system based on EAP and the proposed system with Load Minimization Scheme, in terms of load on the ASN.
- The X-axis represents the Number of Nodes and the Y-axis represents the Number of Packets (load) sent to the tASN.



CONCLUSION

- This system offered minimum load and good performance when measured against the number of nodes and number of handovers.
- It also solved the issue of time-delay by reducing the number of inter-ASN handovers involved.
- Furthermore, our load minimization scheme is found to be more flexible and scalable, whose performance was compared to that of existing systems through simulation.

REFERENCES

- Tarek Bchini, Nabil Tabbane and Sami Tabbane, “Inter-ASN Handover using MSCTP Protocol in IEEE 802.16e Networks”, 2009, *Seventh Annual Communication Networks and Services Research Conference*
- Shaoh-Chen Ke and I-Husan Peng, “A Simplified ASN Anchored Mobility Scheme over Mobile WiMAX”, 2009, *First Asian Himalayas International Conference*
- D.Q.Liu and M.Coslow, “Extensible Authentication Protocols for IEEE standards 802.11 and 802.16”, 2008, pp. 1-9
- Y.Ohba, Q.Wu and G.Zorn, “Extensible Authentication Protocol(EAP) Early Authentication Problem Statement”,2010, *RFC 5836*

....cont.

- Thuy Ngoc Nguyen and Maode Ma, “Enhanced EAP-Based Pre-Authentication for Fast and Secure Inter-ASN Handovers in Mobile WiMAX Networks”, 2012, *IEEE Transactions on Wireless Communications*
- Jozef Kenyeres, Martin Kenyeres, Markus Rupp, and Peter Farkas, “Localized Algorithm for Border Nodes Detection in WSNs”, 2012, *Annual International Conference on Mobile Computing and Networking*

THANK YOU