31st Indian Engineering Congress, Kolkata, 2016
The Institution of Engineers (India)
Theme: SMART Technologies for Natural Resource Conservation and Sustainable Development

Expounding the Complications and Mitigations for Indian Military Force Related Communication Issues

Akarsh Goyal[*1], Nikhil Chaudhari[1], K. Naresh[1] and V. Balasubramanian[1]

Abstract: *Indian military is one of the largest and strongest in the world. It is a very important cog in the wheel for maintaining the welfare and prosperity in the nation. It is because of them that people are able to live at peace in their lush condos while they stand guard at our border 24 × 7. Technology has been a great aid in their functioning. But inspite of so many advances in the science and research, everyday they have to face a myriad of problems. And a lot of these relate to remote communication facilities used by them. So in this paper, focus has been given on communication issues confronted by the army due to the enemies beyond the border line and during natural calamities. The threats due to both of these matters and the most innovative methods related to mobile computing to tackle them are listed here. Also at the end a new model is proposed which would be robust enough to handle these difficulties.*

Keywords: Indian Military, Technology, Enemies, Natural Calamities, Security, Communication.

Introduction

India is a very vast and diverse country with people of all creeds, sects and castes living here. It is very difficult to maintain harmony and peace between so many people who could get incited by raising of a single sensitive issue. Also the country is surrounded by so many neighbours on all sides. Some of them have very cordial relations with India while some on the other hand are quite cold towards it.

Most of the nations look to increase their foothold in the subcontinent by acquiring more area of land from others. This is also done to support their increasing population. But the Indian military force proves to be a deterrent for them. They guard the borders at almost all times of the year even in very harsh conditions are there. Also a major part of the credit goes to them for quelling any internal disturbances within the nation which may be during riots, terrorist attacks or in areas where curfew is nature at their own base as well and also the enemy becoming more intelligent day by day the army needs to up its game. But the technology for logistics and communication used by the army proves to be a hindrance. Much of the equipment used for these purposes have now reached a stage of obsolescence. There is a need to upgrade the remote technologies used by them so as to give them an edge over the difficulties in their path.

So in this paper, the communication problems have been discussed that have been faced by the military due to enemies beyond the line and natural disasters. This paper tried to provide possible solutions related to fields of mobile computing, wireless networks and sensor technology to mitigate them. In addition to it we provide a new holistic proposal which takes into consideration every scenario so as to tackle the issue.

Related Work

A lot of work has been done regarding the communication based security concerns, their solutions, network problems caused by disasters and their mitigations. A few of these elucidated here.

S. Alam [1] worked on wireless sensor network and explained the security threats related to the use of it. In 2004, Perrig *et al*. [2] displayed how major security steps could be implemented in wireless sensor networks and what are the research challenges associated with it. A survey on various aspects connected to ad hoc wireless networks has been performed in [3]. In [4] and [5] all the vulnerabilities, challenges, recent advances and future trends of wireless networks have been elicited. Grover *et al*. [6] have done a case study on jamming and anti-jamming techniques in communication systems. In this paper, jamming has been explained properly and method has been shown that when used effectively could tackle it. In [7] the disaster life cycle has been discussed and how operation research could be applied to it to gain useful insights. Kovács *et al*. identify the different challenges related to human logistics, mainly

[1]*School of Computer Science and Engineering, Vellore Institute of Technology University, Vellore–632014, Tamil Nadu, India.*
✉[*]*akarsh.goyal15@gmail.com*

network systems, in [8] and disaster relief operations to mitigate it in [9]. Various disaster relief operations and resilience systems have been illustrated in [10] and [11] to provide support for a number of disaster organisations working to tackle the calamity problems. In 2015, Pradeep *et al.* [12] have explained the communication networks which could be put to great effect during emergency situations. In [13] a survey on wireless mesh networks has been done. Raniwala [14] have talked about the architecture of multi-channel wireless mesh networks and also have evaluated the performance of various distributed algorithms on the same.

New Proposal for Security against Enemy Beyond the Line Wireless Mesh Networks (WMNs) Integrated with New Security Systems

Here a new wireless mesh network system [13] with new management secured protocols is discussed that will prove very much beneficial for the army. This is because it could be deployed in highly sensitive areas and prove to be a good substitute in place of wireless sensor networks and ad hoc wireless networks which are normally used in military areas.

Architecture

A conventional architecture of a typical WMNS for which we propose a security and privacy protocol. The architecture is a very specific for the army that represents the majority of the real-world deployment scenarios for WMNs [13,14]. The structure of a hierarchical WMN consists of three layers as shown in Figure 1. At the top layers are the Internet Gateways (IGWs) that are connected to the wired Internet. The entities at the second level are called wireless Mesh Routers (MRs) that eliminate the need for wired infrastructure

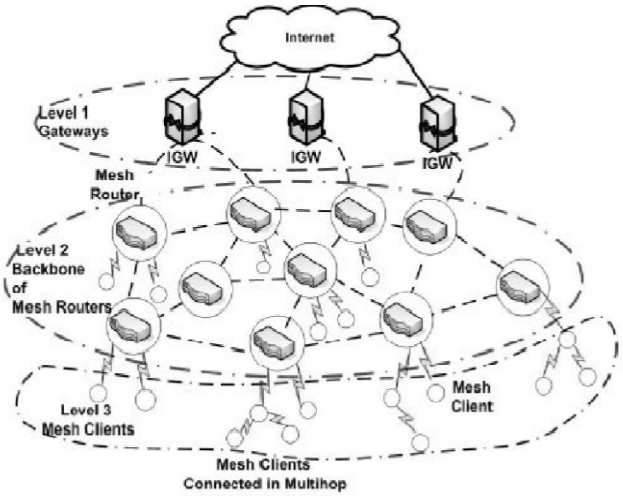

Fig. 1: The Three-Tier Architecture of a Wireless Mesh Network (WMN)

at every MR and forward their traffic in a multi-hop fashion towards the IGW. At the lowest level are the mesh clients (MCs) which are the wireless devices of the users. Internet connectivity and peer-to-peer communications inside the mesh are two critical applications for a WMN. Therefore the design of an efficient and low-overhead communication protocol which ensure security and privacy of the users is an essential requirement which poses significant research challenges.

The proposed security protocol serves the dual purpose of providing security in the access network (i.e., between the MCs and the MRs) and the backbone network (i.e., between the MRs and the IGWs). Hence they could be utilized properly by the army. The dual properties are described the following sub-sections.

Access Network Security

The access mechanism to this new WMN is assumed to be the same as that of a Local Area Network (LAN). This allows the users to access the services of the WMN exploiting the authentication and authorization mechanisms without installing any additional software. It is evident that such security solution provides protection to the wireless links between the MCs and the MRs. A separate security infra-structure is needed for the links in the backbone networks.

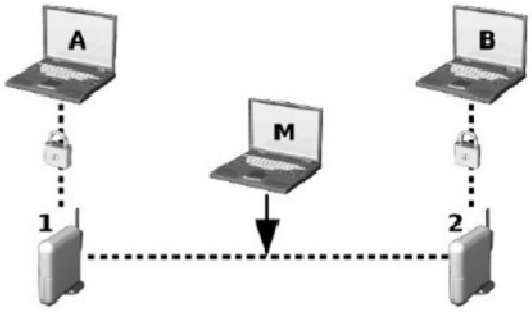

Fig. 2: Secure Information Exchange among the MCs A and B through the MRs 1 and 2

Figure 2 illustrates a scenario where users A and B are communicating in a secure way to MRs 1 and 2 respectively. If the wireless links are not protected, an intruder M will be able to eavesdrop on and possibly manipulate the information being exchanged over the network. This situation is prevented in the proposed security scheme which encrypts all the traffic transmitted on the wireless link using a stream cipher in the data link layer of the protocol stack.

Backbone Network Security

For providing security for the traffic in the backbone network, a two-step approach is adopted. When a new MR [13] joins the network, it first presents itself as an MC and

completes the association formalities. It subsequently upgrades its association by successfully authenticating to the AS. To make such authentication process efficient in a high mobility scenario, the key management and distribution processes have been designed in a way so as to minimize the effect of the authentication overhead on the network performance. The overview of the protocol is shown in Figure 3.

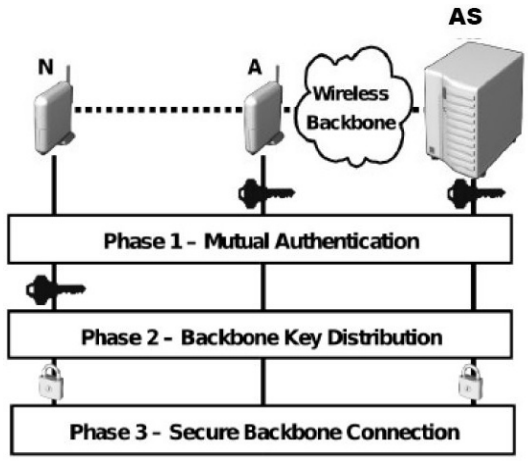

Fig. 3: Steps Performed by a New MR (N) Using Backbone Encrypted Traffic to Join the WMN

The Key Distribution Protocol

In this section, the details of the proposed key distribution and management protocol are presented. The protocol is essentially a server-initiated protocol and provides the clients (MRs and MCs), ie. the army, flexibility and autonomy during the key generation.

Server Initiated Key Management Protocol

In the proposed key management protocol delivers the keys to all the MRs from the AS in a reactive manner.

A newly joined MR, after its successful mutual authentication with a central server, sends its first request for a key list (and its time of generation) currently being used by other existing MRs in the wireless backbone. Let us denote the key list timestamp as TSKL. Let us define a session as the maximum time interval for a validity of the key list currently being used by each node MR and MC). An MR, based on the time instance at which it joins the backbone, can find out the key (from the current list) being used by its peers (key ids) and the interval of validity of the key (Ti) using (1) and (2) as follows:

$$\text{key}_{idx} = \left\lfloor \frac{t_{\text{now}} - TS_{KL}}{\text{timeout}} \right\rfloor + 1 \quad \text{... (1)}$$

$$T_i = \text{key}_{idx} \times \text{timeout} - (t_{now} - TS_{KL}) \quad \text{... (2)}$$

In the proposed protocol, each WMN node requests the AS for the key list that will be used in the next session before the expiry of the current session. This is feature essential for nodes which are located multiple hops away from the AS, since, responses from the AS take a longer time to reach these nodes. So the army personnel stationed at the peak could interact with the base commanders.

In the proposed protocol, the correction factor is estimated based on the time to receive the response from the AS using (3), where ts is the time instance when the first key request was sent, tr is the time instance when the key response was received from the AS, and timeout is the validity period of the key. Therefore, if a node fails to receive a response (i.e., the key list) from the AS [14] during the timeout, and takes a time tlast, it must send the next request to the AS before setting the last key.

$$\begin{aligned} c &= \left\lceil \frac{t_{\text{last}} - \text{timeout}}{\text{timeout}} \right\rceil \quad \text{if } t_{\text{last}} \geq \text{timeout} \\ &= 0 \qquad\qquad\qquad\quad \text{if } t_{\text{last}} < \text{timeout} \qquad \text{... (3)} \\ t_{last} &= t_r - t_s \end{aligned}$$

The first request of the key list sent by the new node to the AS is forwarded by the peer to which it is connected as an MC through the wireless access network. However, the subsequent requests are sent directly over the wireless backbone.

For Mitigating Disasters

Many methods have been explained below which could be used for proper management and relief work during calamity situations faced by Indian army.

Wide Area Disseminator (WAD) Alarm Device

It will be based entirely on widely available mobile communications technologies such as Short Messages and CBM, aimed at rendering a cost effective and reliable mass alert system.

The system is compliant with CAP, which enables the authorized entity to distribute the same warning message to multiple media in one operation.

The block diagram of WAD Device is shown in Figure 4. It comprises of two basic elements – the Server and Clients. The server will reside in a secure facility and will be used by authorized persons to generate warning messages via SMS or CBM. The clients are the intended recipients of the above mentioned messages. Upon reception of the messages the clients will take necessary measures to inform the users. A responsible authority from the relief works would generate an alarm message from which would be received by mobile phones as well as alarm devices.

Once a warning message is received, the (WAD) alarm device responds by either emitting an audible alarm, by flashing a light, or by turning on a radio as directed by the message. The device will also include a call back function, which will allow users to call a dynamic hotline, in order to get more information. SMS-based alerting is used to activate selected alarms/individuals, while the CBM is used to activate all alarms.

The message types employed in the system are two-fold: warning messages, which carry the actual alerts, can either be sent as SMS or CBM. This allows the Alarm to benefit from the advantages of both type of messaging systems for each purpose.

Features of the Device

The overall capabilities of this Alarm Device are as follows:

1. It may be triggered by either SMS or a CBM.
2. Once triggered, the device will display the message on an LCD, emit an audible alarm, flash a light and/ or turn on an in-built radio in response to the trigger.
3. Responds only to warning message in a predetermined format and generated by a recognized source.
4. A hotline number can be sent with message, which the device can dial that number and make a call for more information/instructions.
5. The device is powered from the mains supply under normal operation, includes a backup for operation in the absence of mains power failure and is portable.

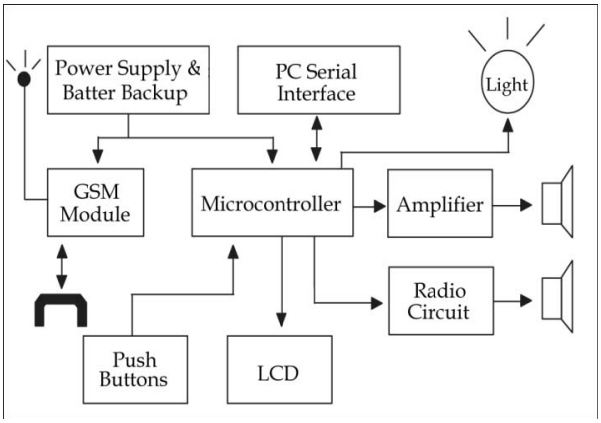

Fig. 4: Block Diagram of the WAD Alarm Device

The microcontroller and the GSM module [8] are the key components of the WAD alarm device. A suitable microcontroller was selected after taking various factors such as reliability, ruggedness, and ease of use. The microcontroller also houses a multitude of peripheral devices such as internal program flash memory, data memory, general purpose I/O, and USARTS.

Once in operation, the GSM module listens for any incoming SMS messages or CBMs. CBM-based warning messages will be broadcast on a predetermined dedicated logical broadcast channel. Upon the reception of a CBM or an SMS, a notification will be sent by the GSM module to the microcontroller. The microcontroller in turn will read and process the message. If the message is from an authorized source such as from military or government organisations (in case of SMS) and conforms to a given format, the WAD alarm device will be triggered he alarm device is designed to power up from the main supply. The device is equipped with a back-up battery as a secondary power source. This battery is capable of powering the device for approximately seven hours. A battery was selected for this purpose after considering the size, cost, durability and maintenance.

The alarm device is designed to power up from the main supply. The device is equipped with a back-up battery as a secondary power source. This battery is capable of powering the device for approximately seven hours. A battery was selected for this purpose after considering the size, cost, durability and maintenance.

The functions of the five push button switches, call, ack, LCD, test and radio are given in Table 1.

Table 1: Functions of Push Buttons on the WAD

Button Name	*Function*
Radio	To turn ON/OFF Radio
Test	To start the test sequence
LCD	To turn ON LCD backlight
Ack	To send acknowledgement (This turns off Alarm and Light)
Call	To call for more information in the event of an emergency (This turns off Alarm and Light)

So this device could prove to be very beneficial in aiding the humongous amount of rescue work undertaken by the army.

Conclusion

The Indian Army shoulders the responsibility of protecting the citizens from various outer and internal encroachments. It goes about its task in a very concise manner. In the face of great adversities as well they display stoicism. But at the end of the day, they are also humans and they cannot always cover their backs. For accomplishing this thing, efficient technology should always be at their disposal. So to give our support to this, two problems, i.e., Security concerns due to enemies and calamities, in specific related to communication which forms an imperative part of the technology used by the Indian military were discussed in this paper. How these two issues could be very much threatening and the ways

which exist to mitigate them are mentioned elaborately here. Also, many new methods are proposed which are highly efficient and cost-effective for mass deployment for use by the army. If these systems are properly implemented, then they can prove to be very advantageous for the military and a deterrent in the path of the enemies of the country.

References

[1] Alam, S. and De, D. (2014). Analysis of security threats in wireless sensor network. arXiv preprint arXiv:1406.0298.

[2] Perrig, A., Stankovic, J. and Wagner, D. (2004). Security in wireless sensor networks. *Communications of the ACM*, 47(6), 53–57.

[3] Singh, R.K., Joshi, R. and Singhal, M. (2013). Analysis of Security Threats and Vulnerabilities in Mobile Ad Hoc Network (MANET). *International Journal of Computer Applications*, 68(4).

[4] Choi, M.K., Robles, R.J., Hong, C.H. and Kim, T.H. (2008). Wireless network security: Vulnerabilities, threats and countermeasures. *International Journal of Multimedia and Ubiquitous Engineering*, 3(3), 77–86.

[5] Zou, Y., Zhu, J., Wang, X. and Hanzo, L. (2015). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends.

[6] Grover, K., Lim, A. and Yang, Q. (2014). Jamming and anti–jamming techniques in wireless networks: A survey. *International Journal of Ad Hoc and Ubiquitous Computing*, 17(4), 197–215.

[7] Altay, N. and Green, W. G. (2006). OR/MS research in disaster operations management. *European journal of operational research*, 175(1), 475–493.

[8] Kovács, G. and Spens, K. (2009). Identifying challenges in humanitarian logistics. *International Journal of Physical Distribution & Logistics Management*, 39(6), 506–528.

[9] Kovács, G. and Spens, K.M. (2007). Humanitarian logistics in disaster relief operations. *International Journal of Physical Distribution & Logistics Management*, 37(2), 99–114.

[10] Luis, E., Dolinskaya, I.S. and Smilowitz, K.R. (2012). Disaster relief routing: Integrating research and practice. *Socio-economic planning sciences*, 46(1), 88–97.

[11] McDaniels, T., Chang, S., Cole, D., Mikawoz, J. and Longstaff, H. (2008). Fostering resilience to extreme events within infrastructure systems: Characterizing decision contexts for mitigation and adaptation. *Global Environmental Change*, 18(2), 310–318.

[12] Pradeep, P.D. and Kumar, B.A. (2015). A Survey of Emergency Communication Network Architectures. International Journal of u-and e-Service, Science and Technology, 8(4), 61–68.

[13] Akyildiz, I.F., Wang, X. and Wang, W. (2005). Wireless mesh networks: a survey. *Computer networks*, 47(4), 445–487.

[14] Raniwala, A. and Chiueh, T.C. (2005, March). Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network. *In Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies* (Vol. 3, pp. 2223–2234). IEEE.