7th International Conference on Recent Innovations in Science, Engineering and Management
The Institutions of Engineers, Delhi State Center (India)
16th September 2016, www.conferenceworld.in
RISEM - 16
ISBN : 978-93-86171-07-8

A STUDY ON MOBILE SECURITY REQUIREMENTS AND CHALLENGES

Milan Singh[1], Deepak Sinwar[2]

[1]PG Student, Department of Computer Science, BRCM College of Engineering and Technology, Bahal, (India)

[2]Assistant Professor, Department of Computer Science, BRCM College of Engineering and Technology, Bahal, (India)

ABSTRACT

Mobile Network is the critical network form defined with specification of dynamic topology and network nodes. This dynamic feature increases the security criticality and results the communication loss. In this paper, the discussion on the security challenges in the network is provided under different aspects. The protocol level, infrastructure level and application specific challenges are discussed. The challenges to the network security with relative communication loss in the network are provided in this paper.

Keywords: *Application Specific, Criticality, Layered Mobile, Security.*

I. INTRODUCTION

A Mobile network is an infrastructure less self organized dynamic network that provides the cooperative communication. Author identified different communication challenges including the security, routing, architectural constraints and the application dependency. The mobility and the dynamic alteration of the network topology is also critical while performing the communication and integrating the security aspects. The primary concern of this network model is to identify the effective network characterization under security concern. Security in this network is provided under various software driven services including the authentication, integrity, availability, anonymity and confidentiality. The security solution and protocol stack specific issue identification was provided for mobile network. The protection against the dynamic behavior and intrusion is the great challenge for mobile network. The potential security constraint analysis can be applied in the network at different levels including the node level observation, cluster specific analysis, mobile agent specific security integration and the infrastructure driven security analysis. The security is also applied at protocol level or the layer specific. This extensive integration is able to provide the reliability enhancement during transmission and while forming the packets. Different security components relative to the mobile network are shown here in Fig.

ISBN : 978-93-86171-07-8

1.

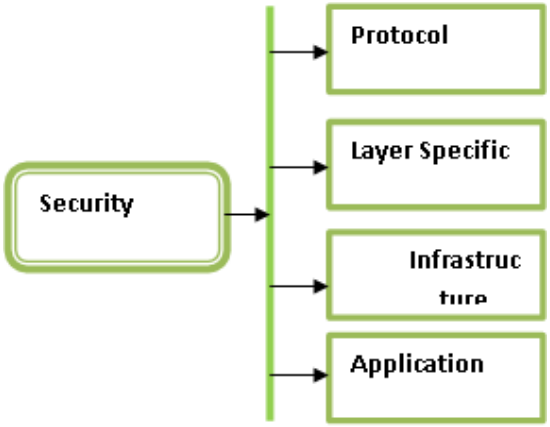

Fig. 1: Security Services In Mobile Network

Here Fig. 1 is showing some of the common security aspects and the observations required for mobile network. The foremost security requirement is at protocol level. The MAC protocol, transport protocol and routing protocols can be improved by security integrity to provide the security at communication time, transportation time and during the packet formation. This kind of security integration does not required specialized infrastructure. Generally authentication driven or the data validation specific security constraints are integrated with the protocol itself. Another type of security constraint defined here is layered services. The communication in the network is formed under different layers specification. Each of the layers is defined with specific role and the integration of security services is required with these roles. The communication control analysis and the packet verification in generic model can be provided by the mobile network. The infrastructure driven security services can be defined by setting up some firewall or including the specialized hardware. This infrastructure can work as the mobile agents or the region specific control. The gateway filtration specific network security integration is also provided for safe network communication. Another security aspect defined here is specific to the application. To provide the security for particular communication type, particular organization or the user group, the security features can be integrated. The organization security integration and enhancement can be achieved by these security prospects. The figure has explored all these constraints that can affect the network security and provides the security at architectural level. This architectural security integration to the mobile network is shown here in figure 2.

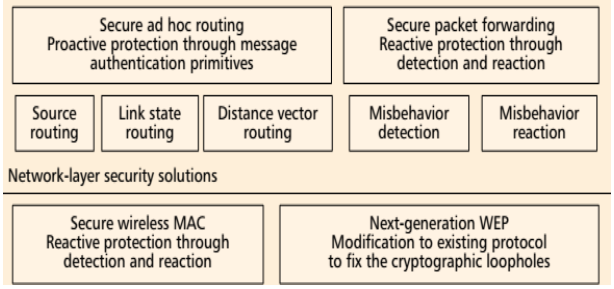

Fig. 2: Type of Security Integration

Here Fig. 2 is showing the different kind of security integrated at different level including the routing aspects and with specification of routing protocol types. This kind of security integration is applied on node selection and cooperative communication formation. The network security features are also defined as the effective security solution. The MAC specific authentication integration is applied to achieve the security at lower level. In this paper, the discussion on the security requires and the challenges exploration is provided.

II. RELATED WORK

A Mobile network is defined in open area with dynamic features including the region switching and new node inclusion. Because of this dynamic nature, the network suffers from various internal and external attacks. Different security features are implied by different researchers in terms of authentication methods, preventive methods as well as attack detection methods. In this work, some of the contributions of different researchers for enhancing the security services in mobile network are presented. M. F. Xue et. al., [1] has defined a security framework to analyze the security threats and requirements in mobile 4G networks. A protocol driven security analysis in secure environment was provided by the author. Author improved the access control mechanism by setting up the trust and validation vector so that the communication reliability will be improved. A trust adaptive security framework was provided by the author. M. Liyanage, [2] has suggested the integration of security services in software defined mobile networks. Author provided the multi-tier security approach to provide the secure communication. The improvement to the protocol is provided by applying the host identity analysis. The unwanted access based address spoofing and the defensive method against DoS attack was provided by the author. The attack mitigation and reliability improvement was suggested by the author. Z. Simate, [3] has integrated the network security and applied its evaluation in GSM enabled mobile network. An association to the network threats and the identification of weak points is provided by the author. Security chain integration and relative threat exploitation was provided by the author. Author identified the security challenges and generated an authentication driven compromising node rectification method for effective network communication. S. Sudin et. al., [4] has work on the security challenges and provided the preventive network communication against popular attacks. A security attributes specific integration and relative risk observation was provided by the author. The attack sensitive risk observation was identified by the author.

M. Seify et. al., [5] has defined a method to reduce the security risk in mobile network. Author defined the risk management mythology to manage the risk and perform the relative evaluation with security policy specification. The threat analysis in GSM enabled network was provided by the author. A distributed asset driven communication with sensitive information processing was provided by the author. A security feature analysis under risk observation was provided by author to reduce the impact of security threats. P. Sharma et. al., [6] has defined a security scheme against the jamming attack for mobile network. The method identified the unauthorized packets and congestion situation to provide the detection of jamming attack. The performance evaluation based multipath routing method is provided for secure communication in mobile network. H. Yang et. al., [7] has discussed the featured constraints against the security criticalities in mobile network. The work was applied on open peer-to-peer architecture so that the resource constraint specific dynamic communication was performed. The security problem estimation with performance and reliability estimation was provided by the author. Dynamic connectivity based security issues were processed by the author to provide layered security

integration so that the communication throughput will be improved. L. Zhang et. al., [8] has defined a work on heterogeneous mobile network with specification of security features and constraints. A protocol specific integration and identification of security issues was provided by the author. The service integration and the protocol driven estimation provided the author to reduce the data transmission and applied the secure handover in the network. The mobility support and security constraint mapping was provided so that effectiveness of network communication will be achieved. S. A. Nargunam et. al., [9] applied the security scheme in clustered mobile network. A unique characterization of security features was provided for shared network for reliable resource allocation. The membership validity based trust evaluation was provided for providing the secure communication in mobile network. A. S. Nargunam et. al., [10] has defined the distributed security mechanism for mobile network so that the architectural challenges will be resolved. Dynamic topology control estimation with security integration was provided so that the layered improvement in the mobile network will be achieved.

M. M. Shurman et. al., [11] has provided the security key based autoconfiguratin method for improving the communication in mobile network. The identity address specific mapping and improvement to the design phase was provided by merging the security constraint to the mobile network. A security key specific significant loss reduction and controlled communication was provided. R. Savola et. al., [12] has defined self measurement based security layered integration to the mobile network. Author identified the security challenges so that the node level and network level reliability will be improved. Independent network estimation under security constraint specification was provided by the author. R. A. Shaikh et. al., [13] has provided the integration of security architecture in multiple hop communication in mobile network. The control security mechanism was suggested using mobile agent integration. The infrastructure specific attack detection method was provided so that the degree of reliability in the network will be improved. R. J. Teke et. al., [14] has defined an enhancement to the mobile mesh network so that the reliability impact of network will be improved. Author applied the attack analysis with connectivity observation and self organizing communication for bait detection scheme. The method identified the black hole nodes and generated the preventive communication route. The self organized structure has provided the network estimation under dynamic constraints so that the reliable network communication will be formed. S. Alampalayam et. al., [15] has discussed the security features under application driven mobile network. The mobility and dynamic aspects along with secure routing method was provided by the author. The security infrastructure inclusion and threat specific communication optimization was suggested by the author. A key pair specific handshaking method was provided to identify different attacks and to provide the safe network communication. Author identified the open communication issues and generated the safe communication route in the network.

D. Dasgupta et. al., [16] has provided the security agent based network security to observe the node level traffic. Author observed the packet, process respective to the user and the system and identified the abnormal communication patterns. Author integrated the intelligent theory using ART2 network as well as applied the fuzzy controller for effective decision making. A profile specific agent was provided to control the communication and to integrate the security aspects to the network. J. Kaur et. al., [17] has provided the improvement to mobile adhoc network by integrating the information security. Author applied the work in JADE environment and enhanced the security constraints with RSA cryptography. A flexible and threat prone

measure was provided by the author to provide environment specific security. The execution model was provided as an extension to improve the multi-security aspect at node level. K. seng Ng et. al., [18] has defined a work to improve the data security and profile specific sharing and communication in mobile network. The dynamic nature of network enforced the security as the challenging issue. A maintenance and effective routing was provided to control the communication using protocols. Author protected the communication for data transmission with higher confidentiality. The work was implemented in realistic environment with dynamic and the environment specific features. K. Parmeswaran et. al., [19] has provided the policy management control system for mobile network. The distributed hierarchical security measure has improved the security portion for adverse conditions including node failure, network partitions, mobility, infrastructure loss, cyber attacks etc. The operational infrastructure and the functioning in the realistic environment were compromised to improve the network communication aspects. The characterization and the dynamic control also improved the preventive strength of the network. C. K. Dimitriadis et. al., [20] has incorporated the specialized devices or infrastructure in core network called Honey net. A feature driven security model without specification of specialized layer was provided. Author defined a threat model to recognize the threat behavior, direction and pattern. Based on this, the service disruption, communication loss and the architectural unbalancing was recognized. The game theory based interaction observation was formalized with specification of mathematical principles. An incident analysis based payoff method was provided to identify the risk situation and provided the potential reliable communication over the network.

B. Sun et. al., [21] has defined a profile based security in mobile network. Author identified the end-to-end security flaws along with potential misbehavior identification. Author identified the masqueraders attack for realistic network and proposed the lotion specific security solution. A feature selection method with traffic pattern observation was provided to identify the misbehaving nodes in the network. M. Renuka et. al., [22] has used the security architecture in integrated form to improve the multi-path cryptography. The parted security was achieved using DSA approach by generating the passive security measure. A secure path model with probabilistic analysis was provided to improve the network communication. R. Savola et. al., [23] has defined the self organized security measure for mobile network. A trust adaptive responsibility analysis was provided under authenticated route transition. The component metric based security was provided against different attacks. H. Yang et. al., [24] has defined a layer specific security model for providing the collaborative security in the mobile network. A cross-validation specific packet forwarding method was defined for preventive measure. The routing message based reactive communication and criteria specification was defined for mobile network. The ticket specific security model was defined with message handshaking. The token revocation was applied to identify the parameter specific effective neighbor. C. Xenakis et. al., [25] has used the privacy branch specific security model for baseband mobile network. Author applied the security using user credential and processed the identify specific communication. The architectural improvement was provided to identify the malware and to provide the safe communication. M. Carvalho et. al., [26] has explored the security features with featured characterization. The shared medium and the collaborative service distribution in secure way were provided by the author. The dynamic nature and the security configuration were applied by the author under aspect derivation. The topological features with frequency range were analyzed by author to avoid the unsafe communication. P. Hari et. al., [27] has provided an innovative approach for reliable and secure mobile

communication. Author has defined the work to analyze the structure for link estimation. The communication pattern on movable nodes is provided for providing the safe communication. E. Gelenbe [28] has defined a work on smart mobile network against various network attacks. Author defined the honey pot based model to analyze the network infrastructure under attack pattern. Author defined the adaptive model for attack detection against various network attacks.

M. J. Peltola et. al., [29] has achieved the public safety and safety for broadband mobile network. Author provided the security solution in real time scenario with specification of sharing constraints. The mobile service distribution and availability was provided to achieve the reliable backup and service distribution. An agent support specific work for security enhancement was provided by J. Zhao et. al., [30]. Author provided the security management and certification using mobile agents. Author also provided the control based communication in regional network. The resource division and security constraint specification was provided at node level. The host level security control was provided to observe the requirement and relatively provided the reliable communication. S. Bu et. al., [31] has defined the intrusion detection and prevention method based on structural analysis. Author provided the activity monitoring using marko decision process to identify the probability of attack in the network. The structural aspect and information state was provided with slot specific observation. The markov model with state observation was provided to control the communication. S. Buchegger et. al., [32] has provided the secure communication routing for mobile network. Author discussed the decision support based analysis to observe the communication behavior with selective network utilization. The protocol resistive security attack was provided to observe the controlled communication. Author provided the security issue specific cooperative communication to provide the distributed communication. The selfish not identification based on behavioral analysis was provided to achieve secure communication. The incentive driven analysis on neighborhood was applied to capture the communication misuse and relatively provided the safe communication. A. Beach et. al., [33] discussed the security and privacy issues as well as identifies the solutions. A secure service transition over compromising nodes was provided by the author for exchanging the information. Author provided the architectural configuration and anomaly detection was provided with high impact.

III. SECURITY CHALLENGES AND REQUIREMENTS

The dynamic mobile network provides the distributed communication and resource allocation and utilization in open network. The application driven requirement analysis and constraint specification is required. The configuration setup as well as to provide the process level communication so that the optimized network communication will be performed. The network is defined with specification various integrated security constraints and challenges. In this section of the associated mobile network challenges and security requirements are discussed.

A. Network Attacks

A mobile network is potentially available in open space so that any existing and new user can participate to the network. The multiple hop communication also includes the intruders as the intermediate node. Because of this, there is the requirement to observe the network connectivity under the layered phenomenon and with

RISEM - 16
ISBN : 978-93-86171-07-8

specification of security constraints. The distributed protocol in the hostile environment can be defined to provide the cooperative network communication so that the safety against various network disruption will be obtained. The network also suffers from different attacks applied by internal and external nodes. The functionality analysis and the packet level analysis are required to provide the safe network communication. The message driven analysis and provides the route specific observation. Some of the common attacks include black hole attack, packet forwarding attack, wormhole attacks etc. These attacks generally disrupt the communication and increase the communication loss.

B. Service Level Challenges

As the network is distributed in the larger network space with specification of large number of network nodes, because of this, there is the requirement to compose the network services in the global environment. The effective service allocation and the service delay is also the challenge for the network. Based on the service type application specification, the load on the network increases. This increased network load also increases the communication delay in the hybrid network environment. Because of this there is the requirement of some aspect specific communication measures so that the adaptive network communication will be formed. The QoS reduction is the security generated criticality in the mobile network.

C. Heavy Traffic

The major aspects of the network are to provide the communication analysis at the switch level and at transportation level. The data forwarding and the communication across the network is also provided. The traditional parameters observation is defined to identify the neighbor nodes if the multiple hop based communication is defined. In such case, the hop specific routing decision can be taken. The shortest path estimation and the border gateway specific protocol map can be defined to generate the communication. The communication strength observation with routing protocol specification is here defined in the switched network to control the latency and the traffic control. The connection modeling and the framework driven communication can be applied. The architecture of the communication can be established for effective communication traffic control so that the safe and the absolute communication will be drawn. The traffic control method with specification of relative data parameters is also defined with forwarding decision so that the controlled communication in switch network will be obtained.

D. Dynamic Route Formation

The route formulation in the mobile network can be done by checking the network connectivity and to provide the layered mechanism to provide the periodic formulation link. The neighbor node analysis and the periodic estimation of the network are provided to generate the optimized network pat. The link estimation and the failure estimation are the key terms to provide the safe communication over the network. The route repair method is here suggested to achieve the link repair specification so that the communication hop driven route discovery is provided. The alternate route formulation and route discovery is here done to improve the network effectiveness. The invalid data communication and the link failure robust communication are required in such networks.

IV. CONCLUSION

A Mobile network is the dynamic public area network that suffers from various network challenges. This paper is focused on security challenges. The security aspect defined here includes against different criticalities including the attacks, service level communication. The paper has identified these challenges under different aspects including the protocol level, layer specific etc.

REFERENCES

[1] M. F. Xue and A. Q. Hu, "A Security Framework for Mobile Network Based on Security Services and Trusted Terminals," 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), Wuhan, 2011, pp. 1-4.

[2] M. Liyanage, "Security for Future Software Defined Mobile Networks," 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, 2015, pp. 256-264.

[3] Z. Simate, "Evaluation of mobile network security," International Conference on Information Science, Computing and Telecommunications, Pan African, Lusaka, 2013, pp. 170-175.

[4] S. Sudin, A. Tretiakov, R. H. R. M. Ali and M. E. Rusli, "Attacks on mobile networks: An overview of new security challenge," International Conference on Electronic Design, Penang, 2008, pp. 1-6.

[5] M. Seify and S. Bijani, "A Methodology for Mobile Network Security Risk Management," 6th International Conference on Information Technology: New Generations, Las Vegas, NV, 2009, pp. 1572-1573.

[6] P. Sharma and A. Suryawanshi, "Enhanced security scheme against Jamming attack in Mobile Ad hoc Network," International Conference on Advances in Engineering and Technology Research (ICAETR), Unnao, 2014, pp. 1-5.

[7] H. Yang, H. Luo, F. Ye, S. Lu and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," in IEEE Wireless Communications, 2004, vol. 11, no. 1, pp. 38-47.

[8] L. Zhang, H. Miyajima and H. Hayashi, "An Effective SIP Security Solution for Heterogeneous Mobile Networks," IEEE International Conference on Communications, Dresden, 2009, pp. 1-5.

[9] S. A. Nargunam and M. P. Sebastian, "Cluster Based Security Scheme for Mobile Ad Hoc Networks," IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, Montreal, Que., 2006, pp. 391-396.

[10] A. S. Nargunam and M. P. Sebastian, "Distributed Security Scheme for Mobile Ad Hoc Networks," IEEE International Conference on Information Acquisition, Shandong, 2006, pp. 166-171.

[11] M. M. Shurman, M. F. Al-Mistarihi and K. A. Darabkh, "Merging dynamic address autoconfiguration and security key protocols in mobile ad hoc networks," 36th International Convention on Information & Communication Technology Electronics & Microelectronics (MIPRO), Opatija, 2013, pp. 441-445.

[12] R. Savola and J. Holappa, "Self-measurement of the information security level in a monitoring system based on mobile ad hoc networks," Proceedings of the 2005 IEEE International Workshop on Measurement Systems for Homeland Security, Contraband Detection and Personal Safety Workshop (IMS), 2005, pp. 42-49.

[13] R. A. Shaikh and Z. A. Shaikh, "A Security Architecture for Multihop Mobile Ad hoc Networks With Mobile Agents," Pakistan Section Multitopic Conference, Karachi, 2005, pp. 1-8.

[14] R. J. Teke, M. S. Chaudhari and R. Prasad, "Impact of security enhancement over Autonomous Mobile Mesh Network (AMMNET)," IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Madurai, 2015, pp. 1-6.

[15] S. Alampalayam, A. Kumar and S. Srinivasan, "Mobile ad hoc network security - a taxonomy," 7th International Conference on Advanced Communication Technology, 2005, Phoenix Park, 2005, pp. 839-844.

[16] D. Dasgupta and H. Brian, "Mobile security agents for network traffic analysis," DARPA Information Survivability Conference & Exposition II, DISCEX '01. Proceedings, Anaheim, CA, 2001, vol.2, pp. 332-340.

[17] J. Kaur, S. Saxena and A. Jain, "Mobile agent information security in ad-hoc network," International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC), Chennai, 2014, pp. 77-80.

[18] K. Seng Ng and W. K. G. Seah, "Routing security and data confidentiality for mobile ad hoc networks," 57th IEEE Semiannual on Vehicular Technology Conference, (VTC-Spring), 2003, vol.3, pp. 1821-1825.

[19] K. Parmeswaran, B. Coan, J. Burns, P. Mouchtaris and S. W. Lucas, "A Distributed Hierarchical Policy Management System for Security Control over Tactical Mobile Ad Hoc Networks," MILCOM 2007 - IEEE Military Communications Conference, Orlando, FL, USA, 2007, pp. 1-9.

[20] C. K. Dimitriadis, "Improving Mobile Core Network Security with Honeynets," IEEE Security & Privacy, 2007, vol. 5, no. 4, pp. 40-47.

[21] B. Sun, X. Jin, Y. Xiao and R. Wang, "NIS07-2: Enhancing Security using Mobility Profile for Cellular Mobile Networks," IEEE Globecom, San Francisco, CA, 2006, pp. 1-5.

[22] M. Renuka and P. Thangaraj, "Multi-path encrypted data security architecture for mobile ad hoc networks," National Conference on Innovations in Emerging Technology (NCOIET), Erode, Tamilnadu, 2011, pp. 153-156.

[23] R. Savola and I. Uusitalo, "Towards Node-Level Security Management in Self-Organizing Mobile Ad Hoc Networks," Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT-ICIW), 2006, pp. 36-36.

[24] H. Yang, J. Shu, X. Meng and S. Lu, "SCAN: self-organized network-layer security in mobile ad hoc networks," IEEE Journal on Selected Areas in Communications, 2006 vol. 24, no. 2, pp. 261-273.

[25] C. Xenakis and C. Ntantogian, "Attacking the baseband modem of mobile phones to breach the users' privacy and network security," 7th International Conference on Cyber Conflict: Architectures in Cyberspace (CyCon), Tallinn, 2015, pp. 231-244.

[26] M. Carvalho, "Security in Mobile Ad Hoc Networks," IEEE Security & Privacy, 2008, vol. 6, no. 2, pp. 72-75.

[27] P. Hari, V. K. Shukla and P. R. Verma, "An innovative approach for security on Mobile Ad-Hoc Network," International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kumaracoil, 2015, pp. 759-765.

[28] E. Gelenbe, "Security for smart mobile networks: The NEMESYS approach," International Conference on Privacy and Security in Mobile Systems (PRISMS), Atlantic City, NJ, 2013, pp. 1-8.

[29] M. J. Peltola, A. University, H. Hammainen and A. University, "Economic feasibility of mobile broadband network for public safety and security," IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, 2015, pp. 67-74.

[30] J. Zhao, C. Yuan and W. Zhang, "Security study of network host supporting Mobile Agent," International Conference on Computer Science and Service System (CSSS), Nanjing, 2011, pp. 2538-2542.

[31] S. Bu, F. R. Yu, X. P. Liu and H. Tang, "Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks," IEEE Transactions on Wireless Communications, 2011 vol. 10, no. 9, pp. 3064-3073.

[32] S. Buchegger and J. Y. Le Boudec, "Nodes bearing grudges: towards routing security, fairness, and robustness in mobile ad hoc networks," 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, Canary Islands, 2002, pp. 403-410.

[33] A. Beach, M. Gartrell and R. Han, "Solutions to Security and Privacy Issues in Mobile Social Networking," International Conference on Computational Science and Engineering, Vancouver, BC, 2009, pp. 1036-1042.