A Pilot Study on Survivability of Networking Based on the Mobile Communication Agents

Awais Akram[1], Ren Jiadong[1], Tahir Rizwan[2], Muhammad Irshad[1],
Sohail M. Noman[1,3], Jehangir Arshad[4], and Sana Ullah Badar[4]
(Corresponding author: Sohail M. Noman)

Department of Computer science and Technology, Yanshan University, PR China[1]
38 Hebei Street West Section, Haigang District, Qinhuangdao, Hebei, China
Department of Automation, Shanghai Jiao Tong University, PR China[2]
Department of Cell Biology and Genetics, Shantou University, Shantou, Guangdong, PR China[3]
Department of Electrical and Computer Engineering, COMSATS University, Pakistan[4]
(Email: mn.sohail@hotmail.com)

(Received Jan. 19, 2020; revised and accepted June 8, 2020)

Abstract

The word coping is characterized as a work-state or a network's ability to provide essential services inside deterministic values. The bulk of networks is unbounded, so they ignore a formal administrative control and have a single security policy framework. Survival training can require such infinite systems to provide essential services while retaining key features, such as privacy, integrity, and efficiency, during failure. The network will adapt and adjust to changes within the network system with self-aware management. This paper outlines the solutions and survival strategies in a network and illustrates how the self-aware architecture handles IPQoS? This significantly discusses the problems of a functioning wireless network and the self-healing methods used in wireless systems.

Keywords: Ad-hoc Routing; Asymmetric Channel; Connectivity and Stability; Low Probability of Detection (LPD); Satellite; Survivability; Wireless Network

1 Introduction

This paper focuses on the survivability of the network infrastructure by considering the detailed revision of various articles on a single platform. In addition, this paper allows the automation of a key network survivability features. The major revised articles includes the theories from Sundeep Selvaraj [33], James Sterbenz *et al.* [37] , Suk Yu Hui *et al.* [15], and Xianghui Liu *et al.* [25]. This paper describes boundaries in a survivable network by modelling of self-healing devices, self-configuration, self-supply, and self-monitoring facilities in the network survivability. The relevant descriptions identify the key characteristics which is accompanied by self-aware management, a policy based QoS management, and strategies to implement future network resources. An agent approach allows building a complex, sophisticated system using modular components and self-aware system can manage the processes itself, which defines different levels, including mediators of access, computer, resource, and network elements. In addition, a survivable wireless network has different challenges as wireless communication travels through an unknown channel, unlike the error free cable distribution. Furthermore, security is essential for survivable networks. This paper also discusses how protection and reliability of a network are preserved.

Network systems have gained drastic significance over the past two decades on different segments of daily life like health, education, travelling, and so on. All these sectors operates and works on the network systems to fulfil their scope globally. Since the network came into reality, people stated realizing about the consequences of network failure which reflect the working habits [10, 38, 39]. Hence, the active precautions came to existence in order to overcome the consequences of critical failure of systems and networks. These overcomes depend on the accurate findings of services in the network on time. Automating these network systems monitoring is critical due to factors like users demand for quality of service, and expense involved in hiring professionals. Therefore, human intervention in network management and process automation is critical which is often called a control plan and management plan. When implementing these strategies, assessing network system operational objectives is very significant which should be allowed with tracking and alteration strategies and techniques [7, 22]. In addition, the network survivability maintenance becomes difficult since the time of global internet services involved. Since central administration is absent, and defense is complicated in an unbounded network. Although such networks lack central administration, but the independent services are more reliable if goes with the proper techniques [2,3,6,38].

2 Designing

The networking environment can be divided into two categories of network infrastructure named bounded and unbounded in creating a survivable framework. Both system parts are regulated and entirely controlled by a single administrative entity in a bounded system, while the unbounded network does not have a centralized control of the system parts [30]. There, the administrative body implies the authority to carry out certain activities in the network rather than a delegate that proposes various solutions.

In addition, the framework is said to have an eternal lifespan in an environment with multiple administrative domains. Online, for instance, can be seen as a boundless environment. The Internet is a collection of many device and network applications. For a public web server, customers in many administrative domains can be available on the Internet. All customers are not regulated fairly by any central authority [21,28]. A web server can therefore never rely on a certain client. In this case, the system is the web server and client. The number of website domains are multiple administrative domains. Most domains have legitimate users, and for anonymous interference, different platforms are used. Such sites cannot be differentiated by their administrative domain but by customer behaviour that is specified by a hypertext transport protocol, a relationship between server and user [2,18,22,27].

Furthermore, the system of web servers and clients is widely distributed across the globe. Legitimate users and attackers are both members of the same community, so it is difficult to isolate those legitimate users from attackers. In other terms, it is quite difficult to attach an area to these legitimate users in a common administrative procedure. Therefore, security is an essential element in the survivable network today.

2.1 Survivable Features of the Network

One of the dominant features of the surviving network is to ensure its survival and to provide essential services, even in case of failure, while preserving other essential properties, such as integrity, secrecy, efficiency and other essential qualities that play an important role in maintaining a balance of multi-quality attributes, such as perforation. The ability of a system to provide essential services while retaining its essential properties continues even if a major portion of the system is not functional. In fact, the next important aspect of their existence is to identify essential services and properties within a specific operating system [5,18,19].

The surviving financial sector maintains integrity, confidentiality and availability, even if an attack/accident causes a certain node or communication connection, of key information such as account and loan information and financial services such as transaction validation and processing. It must be able to retrieve this information and services leaked promptly. The key functionality of the system is to adapt to the environment and provide essential services. The ultimate idea is to carry out the system's task without always creating a functional system component.

2.2 Management Based on Policy

Policy-based administration (PBM) distinguishes knowledge of resource management and information related to the state. This enables an operator to develop coverage objectives and policies that will be followed by potential network infrastructure. Judgment on the resource allocation and configuration can therefore be made locally autonomously. The policy based administration of internet engineering task force (IETF) provides an infrastructure for the management of IP networks with service guarantees. In this context, the technology introduced operates IP networks providing guarantees of service [3,8,23]. In addition, this infrastructure also allows for flexible network conduct.

Further, this reacts differently to different network events based on the defined policy. Such protocols are but a set of rules governing access to network resources and regulating them. It allows network managers or service providers to control their network behaviour based on criteria such as user identity or type of application. Practices at different levels can also be defined. The IETF and DMTF (distributed management task force) develops an alternative significant model called the Policy Core Information Model (PCIM) to see the Network as a state machine using state transition control policies [12,29]. It can identify and monitor states. This model also defines priority roles and the order of performance.

2.3 Agencies Approach

Agency approach is one of the promising features of the survivable network that enables the installation of a complex or sophisticated device with modular components. Intelligent components are often called agents, which are considered to be the core of the multi-agent system. A simple and responsible network process execution software can be used by an agent. It can also have some automatic functional knowledge. Smart agents generally cooperate between user interfaces and smart processes to perform certain common tasks. Agents are therefore accountable for the detection, resolution and infrastructure development as expected. These properties are independent, but also responsible for adapting and distributing networks [20, 35]. The agent-based approach also aims to introduce mobile and responsible agents to deal with the dynamic nature of the network system. The key part of this approach is coordination with other systems and the transfer of research to other intelligent agents to reduce the network connectivity load.

2.4 Self-conscious Infrastructure for Management

The ability to maintain management processes and the associated network infrastructure without some external assistance can be described as self-aware management. The self-conscious management structure includes basic elements such as configuration, optimization, healing, and protection. In fact, self-confident control architecture is built using the concepts of PBM and multi-agent applications [5, 19, 28, 29]. This architecture enables complex service management efficiency within the context. It is also consistent with the IST CADENUS project architecture (creation and deployment of Premium User Services), which consists of access mediators, service mediators, and resource mediators. This standard has established a service level agreement (SLA) on the basis of a three-way framework which includes suitable end-user services [4, 13].

The Access Mediator shall be primarily responsible for the cooperation among end - users and different service providers and shall also have awareness of and conduct end - users, access links and terminal sort in order to access the service provider. In addition, it offers the user a larger choice of services at the lowest cost, simplifying the selection process and informing the user immediately if a new service is convenient.

All new service offers will be notified by the Service Mediator. It is also responsible for maintaining visual access to the resources through a relevant underlying network using the relevant resource mediator. There is no direct contact with the SLA end users by the service mediators. It covers their composition with other service providers and the support of their services with network providers.

The resource mediator manages the network performance according to demand of service providers. The Policy Decision Point (PDP) also plays a role in the policy-based management environment. In addition, the policy of rules to be applied in the network components that are met by the service mediators is identified. The primary role of PDP in this architecture is to send policies to the network level that cannot be implemented directly by network elements. Political rules consist usually of kinds, for, on and on.

2.5 Wireless Networking Should Endure

The environment via which wireless communication travels is unpredictable, unlike error - free transmission. To mention a few environmental radio frequencies, wireless communication may be unreliable due to the noise generated by powerful engines, other wireless devices, microwaves and air moisture content. Wireless networks are manually configurable and follow traditional wired models. This means that it must be programmed to connect the node or transceptors to a specific node, which is usually a central base station. The main challenge is to stop the communication if the node loses contact with its peer. These nodes have been placed in optimal space to compensate for this drawback. But even this decision could not guarantee reliability because the environment today can change [16].

In addition, the most important advances in cellular self - healing was ad hoc networks. They are autonomous, self-organizing and instantly reconfigured without human interference when contact between transceivers fail or break down. These networks can have links or interfaces to other networks such as Ethernet or 802.11 [24]. The key strength of such design is that a base station or central control point is not necessary. Growing node is an endpoint and router for other nodes in the decentralized network. This naturally increases reliability and scalability of the network. Automated analysis by link, road exploration and evaluation of network self - healing algorithms remains the most prominent features. By way of discovery, networks create one or more routes between the sender and the recipient of the message. Throw away route failures, trigger renewed discovery and select the best route for the message through the Evaluation Networks.

Moreover, the wireless network of healing itself is typically pro-active or on-demand, has unique paths and a dynamic routing framework. Such features affect speed, delivery, resource and electricity consumption in different quantities. Continuously updating and reconfiguring positive research networks [11]. They believe that frequent link breaks and changes in performance occur and are structured to continuously explore and strengthen optimum connections. Proactive exploration takes place when nodes assume that each route is viable and try to find it. On request however, the discovery only defines routes that higher-level software requires, allowing the nodes to save bandwidth and resources and preserve the traffic-free network.

Further, sometimes the Dynamic Routing is used to predetermine the end-to-end route and messages are forwarded to all neighbours and transmitted in accordance with a cost scheme. While this routing system has the advantage of several complementary routes from source to end point, it generates much network trade. A gradient routing of Ad - hoc networks means that wireless networks provide full dynamic routing [13]. The routing of GRAd stresses the possibility of redundant routes to maximize the lowest latencies between originators and destinations. GRAd deletes message loops by returning a response to that network traffic when the request reaches the destination. Maintaining multiple routes increases memory costs and network traffic, but flexibility and efficiency in the delivery of messages increase the return.

3 Evaluation

The survival of the network is an important aspect of reliable communication services. Survival consists not only of robustness against natural failures, accidents or unintended operational errors, but also of failures due to malice, especially in the context of military networks. Cell wireless networks provide ubiquitous computing and unthread Internet access, but they pose a significant challenge to survival both because users are cell and communications accessible to everyone [34]. This segment also discusses the problems, obstacles and research proposals in cellular sustaining networks as a consequence of our participation in a study program of DARPA's Mobile Wireless Information Networks.

3.1 Resilience, Regeneration, Appreciation, and Reconstruction

Survival focuses on the delivery and maintenance of essential services. Essential services and equipment are the device features necessary to the accomplishment of mission objectives. Resistance, recognition and rehabilitation depend on three key abilities. Resistance is the ability of a system to repel attacks. Recognition is the ability to detect attacks, assess damage and compromise and recovery characteristics, the ability to provide essential services and assets for attacks, to limit damage levels and to restore full post - attack services. We extend this definition further to require survivable systems to quickly incorporate lessons from failures, develop and adapt to emerging threats [4, 12]. We call this a refinement of survival. We may categorize survivable wireless networking specifications into four categories, including opposition, identification, recovery and enhancement requirements.

Moreover, the survival criterion can be defined as a specification technique based on software requirement definition processes. This includes identifying program and security criteria, permissible and invasive applications, development needs, operational requirements and evolution criteria. Essential services and resistance, identification and recovery requirements must be established for entry, exploration and exploitation phases of the assault. Both methods have driven the research and are proposed for further study of mobile wireless networks in the future [13]. Finally, two distinct aspects of sustainability span all networking levels. One is access to information and the second is contact from end-to-end.

The customer would accept obtaining information or services required to complete the task in the event of failure or assault in the event of access requirements. For example, when the network is partitioned, will services or information be replicated and distributed locally? End-to-end interactions should not be expected in these circumstances. In addition, interactive applications and interpersonal communications such as voice calls or dynamically generated information are available in the context of end-to-end communication requirements. Are current sessions surviving? Does the user should create new sessions to reach the desired point of contact even with crashes and attacks? It requires protection of the communication endpoints, and the adversary cannot divide the network indefinitely. In addition, the opponent cannot permanently disable access to necessary services, such as routing, authentication, discovery of resources or naming.

3.2 Military and Cellular Network Survivability

In order to support military operations, use of Wireless Networking technologies imposes strict security and operational obligation on technology such as Transmission Safety (TRANSEC, COMSEC), Authorization and Access Controls, Network Infrastructure Safety, Robustness and Performance. Furthermore, the current work on cell phone network survival focuses mainly on infrastructure survival and does not take into account adversarial attacks. They provide insight into the survival quantification and function of network management tools. Networks, especially software, are vulnerable during upgrades [9,17,31]. Therefore, rapid evolution leads to learning curve problems and over-concentration of traffic or services in single failure points.

Moreover, deficits of operating and maintaining increasingly complex systems in network management tools exacerbate this problem. Deployment failures (for example, fiber backup circuits) will deactivate fault tolerance designs. The use of reliable networks (e.g. SONET-rings), multi-mode systems, and overlay networks to improve survival requires cell technological improvements [1, 24]. Historically, fixed and wireless providers were various administrative bodies, and the reliability of radio links was poor and low expectations increased. Reliability and survival issues will become increasingly important in future cellular networks.

4 Wireless AD-HOC Network Safety

4.1 Connectivity Protections

The first big survival goal is to establish and sustain a network as shown in the Figure 1, where possible. This allows traditional routing and end-to-end protocols to be carried out. The goal is to stay steady [26, 40, 41].

4.2 Foundation Assumptions

There are two separate forms of thought about the area of all-round wireless networking. One approach (for example, Mobile IP) often depends on pre-configured networks. The other (ad-hoc networks) solution suggests that all nodes operate a common ad hoc routing protocol and that there are no networks. There is a small mix of heterogeneous wired and wireless networks. The practice

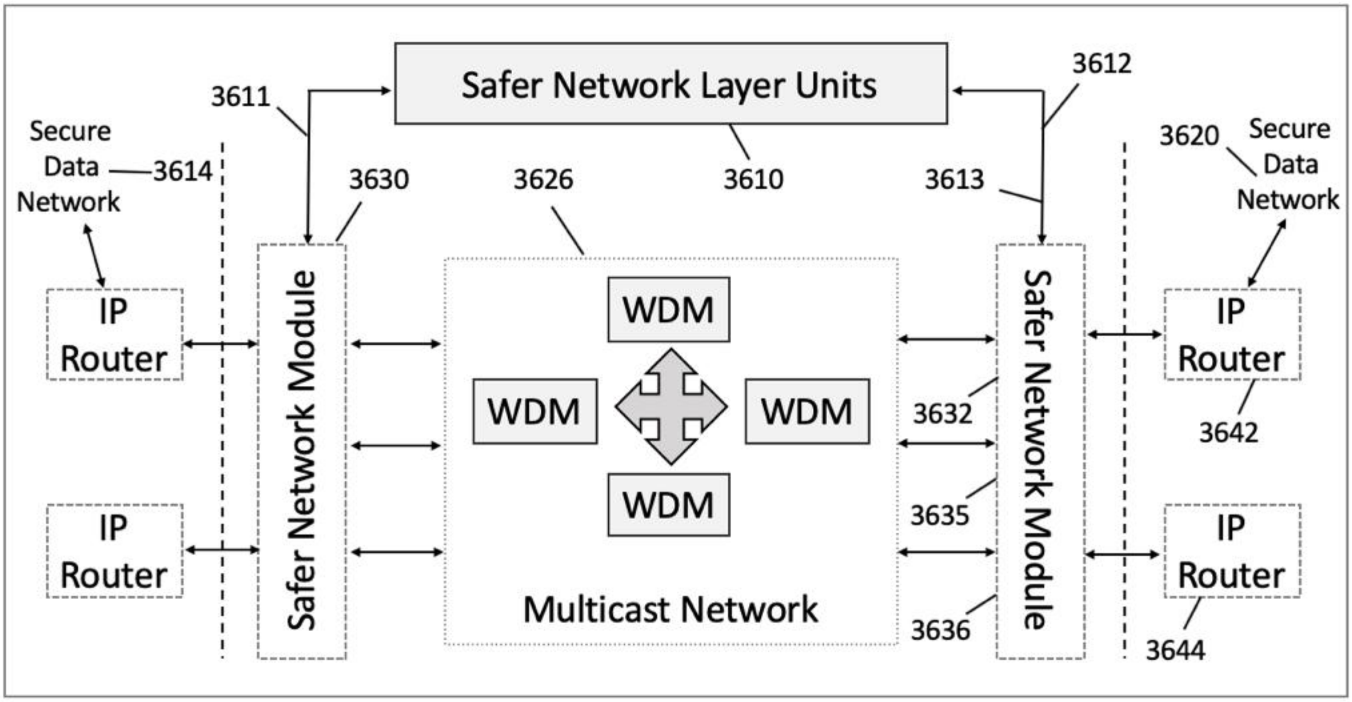

Figure 1: Survivable connectivity flow structure

of quasi-static naming of nodes and subnetworks on IP networks is one justification [32,36].

In addition, the exploration and self-configuration of current networks is not feasible with new technologies. In any research system, mechanical fullback modes that enable ad-hoc networking of the nodes of Internet terminals do not exist. Such a multimodal service is essential for survivable mobile networking, which has an efficient and smooth transition between basic ad-hoc and infrastructure modes [41]. By seamlessly transportation and application sessions must survive switching between infrastructure and ad-hoc modes.

4.3 Auto-configuration Network Layer

Most self-configuration research is about naming and device creation in heterogeneous networks. They presume that each network node has both an address and a routing scheme in advance. This affects overlays at application level rather than network bootstrap. Wired network self-configuration is usually limited to a DHCP, Zeroconf, or existing unique host identification system such as IPv6 [14]. Such approaches and strategies involve unique resources or network identifiers. Surviving nodes must address the problem of auto-configuring mission-based naming, routing and signalling in secure network layer. Safe wireless network automated configuration remains complex because no suitable approaches except for address-less routing approaches such as diffusion routing for specific applications and single shared, probabilistic or gossip-based protocols are established. There is need of establishing further studies in this scope.

4.4 Private Sensor Network

Many ad-hoc networks that already exist do not require private nodes. For each node it assumes unique identifiers such as the Ethernet MAC address or IPv6 EUI-64 identification. Common identities present other concerns about health and confidentiality. Knowing an identifier of a node does not necessarily reveal the identity of the user or owner, but may provide hints that pose unacceptable risks for topology or traffic analysis. An anonymous network cannot determistically assign global unique IDs. The only way to avoid this is to specify an initiator or to allow random ties. There may be some clustering strategies for certain methodologies, such as amorphic calculation, anonymous address networks and spare wireless networks [34].

4.5 Statistical Odds of Detection

The low probability of detection, interception and misuse of (LPD/LPI/LPE), that is a capability of an enemy to monitor and manipulate radio energy, is paramount for most ad - hoc strategic networks. Few techniques can be used to obscure the radio signature of a node, including hidden waveforms, space diffusions and lower transmitter capacity. Survival increases as the network becomes rugged to future opponents. But it makes legal interactions more difficult; lower transmission power generally increases the probability of detection of both enemies and valid nodes [13]. In fact, strategic networks must be able to deny topology information to opponents.

5 Discussion and Potential Direction

This section describes two technologies, include centered drivers for the adaptation and connection of adaptive and satellite networks with a view to dynamic environments. This eliminates the need for standardization and determination of the full range of algorithms, protocols and hard code in nodes prior to deployment. Only a structure for the exploration of nodes and protocol agreements must be established beforehand; radio software is a key technology.

Despite the standardization and pre-known program, application and task conditions, mobile wireless networks are inherently complex and allow for volatile channel conditions. So, network nodes and protocols that learn and adapt to their environment are required for surviving networks. The next step is semantic networking, allowing potential nodes and networks to know about their environment and to take measures to improve sustainability. In addition, the effects of weakly linked channels and node mobility can be minimized by satellites and UAVs. Satellites and other airborne nodes offer unique features similar to ground-based nodes. The high altitude of a satellite allows a very large terrestrial footprint where every ground node can communicate and communicate optionally to the satellite.

Furthermore, this benefit, together with the so called intrinsic transmit power of the satellite, allows the satellite to connect to a large number of earth nodes, providing a broader spectrum than earth nodes. A satellite occurs at a predetermined space point at a mobile node. Satellites are geostationary (GEO), whereas small satellites (MEO) and low-earth satellites (LEO) have computerized trajectories. UAVs may have predictable pathways (e.g. shape of tracks). Where satellite footprint represents cluster or cell size, handovers between node and satellite are more uncommon than between ground-based node and base station, while gaps in retrieval and registration are minimised. The altitude that protects the satellite from overrunning (physical attack) also restricts node mobility.

In particular, survivable networks require more than conventional reliability and fear to loss. While considerable progress has been made on the creation and maintenance of connected networks, further research is required to understand trade-offs towards stealth criteria (LPI/LPD/LPE). In addition, surviving mobile wireless networks require that asymmetric, weakly connected and episodically disconnected links are not defects, but first class citizens. Agility is also essential and used to improve survival. We suggest a significant improvement in how routing algorithms manage communication, encouraging potential networking in areas where this is not currently possible.

In addition, research has begun to scratch the surface because it is not possible or practical to a priori to anticipate the contact environment. It is important that network nodes and protocols respond to their communication scenario or tasks. Dynamically flexible protocols, algorithms and parameters using active networking and software radio technology are key enablers for this functionality. Aerial nodes like satellites and UAVs also provide innovative networks in order to alleviate the impacts of isolated and asymmetric connections and mobility. Moreover, the problems of 5G network testing are identified and defined. Problems as the machine, telecommunications and services are grouped into three regions. Some challenges, including multimode terminals, wireless system discovery, application compatibility and QoS support, are well explored. Nevertheless, some are less known. These include selection of systems, stability, breakdown and life. Research is also required in 5G networks to incorporate personal independence, billing and accounting structures. The discussion in this article not only demonstrates that much work needs to be done of terms of transitioning to 5G systems but also illustrates the need to incorporate current systems so that 5G technology can be implemented smoothly. 5G networks will not start quickly without these infrastructures.

6 Conclusions

To sum up, the results from recent studies, including modelling various self-healing devices to assess serviceability, QoS guarantees for self (configuration, supply, and monitoring facilities), are reviewed in this paper. The theory of agents described in this paper allows automation a key element of survivable networks. Notwithstanding efforts to maintain safety in unlimited networks, the preservation ethos contributes to tightening security in unlimited networks. Survivable Network also has interesting areas for further research.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] S. E. Abkari, A. Jilbab, and J. E. Mhamdi, “Wireless indoor localization using fingerprinting and trilateration,” *IJCSNS International Journal of Computer Science and Network Security*, vol. 20, no. 5, p. 131, 2020.

[2] R. S. Alonso, I. Sittón-Candanedo, S. Rodríguez-González, Ó. García, and J. Prieto, “A survey on software-defined networks and edge computing over

iot," in *International Conference on Practical Applications of Agents and Multi-Agent Systems*, pp. 289–301, 2019.

[3] J. Arshad, S. Salim, T. Younas, M. D. Amentie, G. Farid, A. U. Rehman, and A. Khokhar, "A study on device automation: An integration of internet protocols and embedded system," in *International Conference on Engineering and Emerging Technologies (ICEET'20)*, pp. 1–6, 2020.

[4] O. Awotayo, "Information systems strategies for small and medium size enterprise sustainability," *Walden University*, 2020. (https://search.proquest.com/openview/9f61763613d800f87a620cdc68d0933b/1?pq-origsite=gscholar&cbl=18750&diss=y)

[5] P. Baumann and M. M. Keupp, "Assessing the reliability of street networks: A case study based on the swiss street network," in *The Security of Critical Infrastructures*, pp. 111–129, 2020.

[6] L. Deng, D. Li, X. Yao, D. Cox, and H. Wang, "Mobile network intrusion detection for iot system based on transfer learning algorithm," *Cluster Computing*, vol. 22, no. 4, pp. 9889–9904, 2019.

[7] J. Dong, G. Wu, T. Yang, and Z. Jiang, "Battlefield situation awareness and networking based on agent distributed computing," *Physical Communication*, vol. 33, pp. 178–186, 2019.

[8] A. M. F. Durrani, A. U. Rehman, A. Farooq, J. A. Meo, and M. T. Sadiq, "An automated waste control management system (AWCMS) by using arduino," in *International Conference on Engineering and Emerging Technologies (ICEET'19)*, pp. 1–6, 2019.

[9] E. Felemban, "Passively inferring wireless network signal quality from different data resources," *IJCSNS International Journal of Computer Science and Network Security*, vol. 20, no. 5, p. 138, 2020.

[10] R. Fotohi, E. Nazemi, and F. S. Aliee, "An agent-based self-protective method to secure communication between UAVs in unmanned aerial vehicle networks," *Vehicular Communications*, p. 100267, 2020.

[11] E. N. Ganesh, "Study of voip network delay using neural networks," *International Journal of Electronics Engineering*, vol. 12, no. 2, pp. 83–91, 2020.

[12] W. Han and C. Lei, "A survey on policy languages in network and security management," *Computer Networks*, vol. 56, no. 1, pp. 477–489, 2012.

[13] B. Harris, "Survival and sustainability for small businesses within the timber industry," *Trident University International, ProQuest Dissertations Publishing*, 2020. (https://search.proquest.com/openview/c8f076325516acb18a76c444a180d9f7/1?pq-origsite=gscholar&cbl=18750&diss=y)

[14] G. Howser, "The network layer," in *Computer Networks and the Internet*, pp. 55–87, 2020.

[15] S. Y. Hui and K. H. Yeung, "Challenges in the migration to 4G mobile systems," *IEEE Communications Magazine*, vol. 41, no. 12, pp. 54–59, 2003.

[16] S. Islam, H. Ali, A. Habib, N. Nobi, M. Alam, and D. Hossain, "Threat minimization by design and deployment of secured networking model," *International Journal of Electronics and Information Engineering*, vol. 8, no. 2, pp. 135–144, 2018.

[17] J. Jabbar *et al.*, "Socialize the behavior of iot on human to devices interaction and internet marketing," *IJCSNS International Journal of Computer Science and Network Security*, vol. 20, no. 5, pp. 158–164, 2020.

[18] M. A. Kochte, R. Baranowski, M. Sauer, B. Becker, and H. J. Wunderlich, "Formal verification of secure reconfigurable scan network infrastructure," in *The 21th IEEE European Test Symposium (ETS'16)*, pp. 1–6, 2016.

[19] M. Kountouris *et al.*, "Performance limits of network densification," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 6, pp. 1294–1308, 2017.

[20] D. Kumar, A. Sharma, R. Kumar, and N. Sharma, "A holistic survey on disaster and disruption in optical communication network," *Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering)*, vol. 13, no. 2, pp. 130–135, 2020.

[21] M. Lecuyer, V. Atlidakis, R. Geambasu, D. Hsu, and S. Jana, "Certified robustness to adversarial examples with differential privacy," in *IEEE Symposium on Security and Privacy (SP'19)*, pp. 656–672, 2019.

[22] G. Leu and J. Tang, "Comparison of infrastructure and adhoc modes in survivable networks enabled by evolutionary swarms," in *International Conference on Swarm Intelligence*, pp. 80–89, 2019.

[23] D. Li, R. Zhang, S. Jia, D. Liu, Y. Jin, and J. Li, "Improved dynamic frequency-scaling approach for energy-saving-based radial basis function neural network," *IET Cyber-Physical Systems: Theory & Applications*, vol. 5, no. 2, 2020.

[24] L. Liu, L. Wang, and Z. Cao, "A note on one adaptive indexing structure for realtime search on microblogs," *International Journal of Electronics Engineering*, vol. 12, no. 1, pp. 1–6, 2020.

[25] X. Liu, J. Ning, J. Li, J. Yin, and M. Li, "Model for survivability of wireless sensor network," in *International Conference on Mobile Ad-Hoc and Sensor Networks*, pp. 705–714, 2007.

[26] Y. Liu, J. Bi, and J. Yang, "Research on vehicular ad hoc networks," in *Chinese Control and Decision Conference*, pp. 4430–4435, 2009.

[27] S. H. Mohamed, T. E. H. El-Gorashi, and J. M. H. Elmirghani, "A survey of big data machine learning applications optimization in cloud data centers and networks," *Networking and Internet Architecture*, 2019. (https://arxiv.org/abs/1910.00731)

[28] D. Mox, M. Calvo-Fullana, J. Fink, V. Kumar, and A. Ribeiro, "Mobile wireless network infrastructure on demand," *Robotics*, 2020. (https://arxiv.org/abs/2002.03026)

[29] R. Nabhen, E. Jamhour, and C. Maziero, "RBPIM: A PCIM-based framework for RBAC," in *Proccedings of the 28th Annual IEEE International Conference on Local Computer Networks (LCN '03)*, pp. 52–61, 2003.

[30] S. O. Obute, M. R. Dogar, and J. H. Boyle, "Chemotaxis based virtual fence for swarm robots in unbounded environments," in *Conference on Biomimetic and Biohybrid Systems*, pp. 216–227, 2019.

[31] K. Odagiri, S. Shimizu, and N. Ishii, "Implementation of user authentication processes for the cloud type virtual policy based network management scheme for the specific domain," *IJCSNS International Journal of Computer Science and Network Security*, vol. 20, no. 5, pp. 197–204, 2020.

[32] H. A. Omar, N. Lu, and W. Zhuang, "Wireless access technologies for vehicular network safety applications," *IEEE Network*, vol. 30, no. 4, pp. 22–26, 2016.

[33] S. S. Pundamale, "Survivable networks," *Department of Computer Science, University of Helsinki*, vol. 2, 2007. (`https://www.cs.helsinki.fi/u/niklande/opetus/SemK07/paper/pundamale.pdf`)

[34] M. Sakib and J. Singh, "Simulation based performance analysis of IPSec VPN over IPv6 networks," *International Journal of Electronics Engineering*, vol. 12, no. 2, pp. 92–104, 2020.

[35] L. B. L. Santos, L. R. Londe, T. J. D. Carvalho, D. S. Menasché, and D. A. Vega-Oliveros, "About interfaces between machine learning, complex networks, survivability analysis, and disaster risk reduction," in *Towards Mathematics, Computers and Environment: A Disasters Perspective*, pp. 185–215, 2019.

[36] A. Sharif, J. P. Li, M. A. Saleem, T. Saba, and R. Kumar, "Efficient hybrid clustering scheme for data delivery using internet of things enabled vehicular ad hoc networks in smart city traffic congestion," *Journal of Internet Technology*, vol. 21, no. 1, pp. 149–157, 2020.

[37] J. P. G. Sterbenz, R. Krishnan, R. R. Hain, A. W. Jackson, D. Levin, R. Ramanathan, and J. Zao, "Survivable mobile wireless networks: Issues, challenges, and research directions," in *Proceedings of the 1st ACM Workshop on Wireless Security*, pp. 31–40, 2002.

[38] J. Tang and G. Leu, "Survivable networks via online real-time evolution of dual air-ground swarm," *Swarm and Evolutionary Computation*, vol. 53, pp. 100642, 2020.

[39] V. T. Venkateswarlu, P. V. Naganjaneyulu, and D. N. Rao, "Rendezvous agents-based routing protocol for delay sensitive data transmission over wireless sensor networks with mobile sink," *International Journal of Intelligent Enterprise*, vol. 7, no. 1-3, pp. 338–355, 2020.

[40] Y. Ye, S. Feng, M. Liu, X. Sun, T. Xu, and X. Tong, "A safe proactive routing protocol sdsdv for ad hoc network," *International Journal of Wireless Information Networks*, vol. 25, no. 3, pp. 348–357, 2018.

[41] S. Yousefi, M. S. Mousavi, and M. Fathy, "Vehicular ad hoc networks (vanets): Challenges and perspectives," in *The 6th International Conference on ITS Telecommunications*, pp. 761–766, 2006.

Biography

Awais Akram was born in Pakistan and holds a Bachelor's degree (B.Sc) and Master's degree (M.Sc) in Computer Science from the Islamic University of Bahawalpur, Pakistan. Currently, he pursuing a Ph.D. research at "Yanshan University, China" with projects related to "Network Security and Complex Networks."

Ren Jiadong received the B.S. and M.S. degrees from the Northeast Heavy Machinery Institute, in 1989 and 1994, respectively, and the Ph.D. degree from the Harbin Institute of Technology, in 1999. He is currently a Professor with the School of Information Science and Engineering, Yanshan University, China. His research interests include data mining, complex networks, and software security.

Tahir Rizwan was born in Pakistan in 1987 and earned his B.Sc. degree in "Electrical and Electronic Engineering" from the University of Sunderland, UK in 2012. In 2015, author completed his Master's Degree at "Xidain University, China" in the framework of various projects. The author is currently pursuing a Ph.D. research in "Control Science and Engineering" from "Shanghai Jiao Tong University, China" with the participation of "Artificial Intelligence, Control Theory, Swarm Robots, Machine Learning, Semantic Segmentation and Networking" projects.

Muhammad Irshad He was born in Pakistan and graduated from "University of Punjab, Lahore, Pakistan." Currently, the author is doing a Ph.D. research in "Computer Science and Technology" at "Yanshan University, China" with a project called "Data Mining and Analysis, Networking and Software Security."

Sohail M. Noman received his B. Sc. (Hons) and M. Sc. from University of East London, UK in 2012 and 2014, respectively, and the Ph.D. degree from the Yanshan University, China, in 2020. He is currently pursuing a Post-Doctoral Research fellowship with Shantou University Medical College, China. His research interests include Computer Sciences and Information Technology, with exposure to Healthcare, Data mining, Bioinformatics, and Market Research.

Jehangir Arshad received his Bachelor's degree in Computer Engineering from COMSATS University of Islamabad, Lahore Campus, Pakistan in 2010 and his Master's degree in Electrical and Electronics Engineering from the School of Electronics Engineering, Bradford University, England in 2012. He worked as a lecturer at COM-

SATS Islamabad University, Sahiwal Campus, Pakistan from 2012 to 2017. After completing his Ph.D. studies at the State Key Laboratory of Integrated Service Networks, Xi'an, China University, he joined COMSATS as an Assistant Professor in July 2017. His research interests include the Wireless Communications Network, Network Security and User Authentication, 5th Generation Mobile Communication Systems and alternative energy systems.

Sana Ullah Badar holds a Bachelor's degree in Computer Science from NFC IET Multan , Pakistan in 2013 and a Master's degree in Computer Science from Government College Lahore , Pakistan in 2016. Since 2017, he has worked as a lecturer at COMSATS University of Islamabad, Sahiwal Campus, Pakistan. In parallel, he is pursuing Ph.D. in Computer Sciences. His research interests include Network Security and User Authentication, Data Science, Big Data, and alternative energy systems.