

## Research Article

# A Crowd-Based Intelligence Approach for Measurable Security, Privacy, and Dependability in Internet of Automated Vehicles with Vehicular Fog

Ashish Rauniyar <sup>1,2</sup>, Desta Haileselassie Hagos <sup>1,2</sup> and Manish Shrestha <sup>1,3</sup>

<sup>1</sup>Network and Distributed System (ND) Research Group, Department of Informatics, University of Oslo, Oslo, Norway

<sup>2</sup>Autonomous Systems and Networks (ASN) Research Group, Department of Computer Science, OsloMet-Oslo Metropolitan University, Oslo, Norway

<sup>3</sup>eSmart Systems, Halden, Norway

Correspondence should be addressed to Ashish Rauniyar; ashish.rauniyar@hioa.no

Received 21 June 2017; Revised 11 October 2017; Accepted 9 January 2018; Published 1 March 2018

Academic Editor: Claudio Agostino Ardagna

Copyright © 2018 Ashish Rauniyar et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the advent of Internet of things (IoT) and cloud computing technologies, we are in the era of automation, device-to-device (D2D) and machine-to-machine (M2M) communications. Automated vehicles have recently gained a huge attention worldwide, and it has created a new wave of revolution in automobile industries. However, in order to fully establish automated vehicles and their connectivity to the surroundings, *security*, *privacy*, and *dependability* always remain a crucial issue. One cannot deny the fact that such automatic vehicles are highly vulnerable to different kinds of security attacks. Also, today's such systems are built from generic components. Prior analysis of different attack trends and vulnerabilities enables us to deploy security solutions effectively. Moreover, scientific research has shown that a "group" can perform better than individuals in making decisions and predictions. Therefore, this paper deals with the measurable *security*, *privacy*, and *dependability* of automated vehicles through the *crowd-based intelligence approach* that is inspired from *swarm intelligence*. We have studied *three* use case scenarios of automated vehicles and systems with vehicular fog and have analyzed the *security*, *privacy*, and *dependability* metrics of such systems. Our systematic approaches to measuring efficient system configuration, *security*, *privacy*, and *dependability* of automated vehicles are essential for getting the overall picture of the system such as design patterns, best practices for configuration of system, metrics, and measurements.

## 1. Introduction

Internet of things (IoT) is one of the recent research topics and has attracted a huge attention from academia and industry across the globe. Due to these IoT technologies supported by cloud computing infrastructures, we are living in the smart era where a large number of smart devices ranging from home appliances to outdoor environmental monitoring systems are making our life simple, meaningful, and yet exciting on a day-to-day basis [1]. With the advancement of technologies, automation, device-to-device (D2D) and machine-to-machine (M2M) communications, is fully possible without any human intervention. The automated vehicle is one of the technologies supported by IoT

for smart mobility. An automated vehicle is a vehicle that is capable of sensing its environment through numbers of on-board sensors and navigating on the roads without any human inputs [2]. Radar, laser light, global positioning system (GPS), sensing system, odometry, computer vision etc., are some of the technologies used by autonomous vehicles to detect their surroundings [3]. Major car companies such as *Volvo*, *Toyota*, and *Ford* have already announced that within the next five years their fully automated (autonomous) vehicles will hit the market creating a new wave of revolution in automobile industries. Many high-tech leading companies such as *TESLA*, *Google*, and *UBER* are also working on automated vehicles and cars to bring the idea of smart mobility in practice as soon as possible. It is

envisioned that automated vehicles will reduce traffic congestion, create efficiency, increase safety, save consumers money, and enhance mobility for children, elderly, and disabled people [4]. Considering the large number of sensors required for successful operation of automated vehicles, huge amount of data traffic is expected. The data also need to be processed quickly so that effective decision can be taken by the automated vehicles running on the roads. The data traffic of automated vehicles in IoT environment can be classified as follows [5]:

- (i) *Traffic class 1*: it is a data traffic generated by periodical update or time-based updates by different sensors and applications.
- (ii) *Traffic class 2*: it is a data traffic generated by unexpected events. Whenever there is a sudden or unexpected event, data is generated.
- (iii) *Traffic class 3*: it is a data traffic generated due to a query from applications. Whenever there is a query from applications, data is generated in response to the query.

*Traffic class 1* and *traffic class 2* come under *PUSH* traffic where data is pushed into the cloud based on periodical update or triggered by the events. *Traffic class 3* comes under *PULL* traffic where data is pulled from the cloud in response to the query from the applications of automated vehicles. A traffic class is important for automated vehicles as it can help to counterattack security and privacy issues in such automated vehicles.

With the advancement of technologies, today's modern systems are no longer deployed as separate systems, but the trend is moving towards connecting everything via heterogeneous interfaces and networks. Also, today's systems are built from generic components. Prior analysis and affirmation of different attack trends and vulnerabilities enable us to deploy proactive and security solutions effectively. Undoubtedly, IoT is booming and bringing smartness to all of our lives. Systematic approaches to measure efficient system configuration, *security*, *privacy*, and *dependability* of such IoT systems are essential for getting the overall picture of the system such as design patterns, best practices for configuration of system, metrics, measurements, and so on. Bécsi et al. have claimed that the introduction of connectivity in cars introduces the vulnerabilities and suggests the need of ICT security into the vehicles [6]. It points out the areas of concerns to protect the connected vehicles from security threats. It has considered the under-the-hood components like engine control units (ECUs), vehicular network, and gateway as major points of attacks in any connected vehicles. Moreover, rooting and jailbreaking of mobile devices also increase vulnerabilities of connected cars. In addition to this, the authors have studied the security of connected vehicles in simulated environment shows several attack scenarios in different network layers and its impact on the Cooperative Adaptive Cruise Control (CACC). They have also provided in their work the countermeasures to improve the security and safety of connected vehicles. Koscher et al. have experimentally demonstrated the vulnerabilities in modern

automobiles launching several attacks by getting into cars internal network and having control over all computer control systems including brakes and engines [7]. So, autonomous vehicles have several security and privacy challenges that need to be properly addressed. An approach for measurable security has been utilized in the European Dependable Embedded Wireless Infrastructure (DEWI) security project which proposed the metrics for measurable security in cyber-physical systems in automotive domain [8]. It is based on the European SHIELD approach [9] of dividing a system into subsystems and components and evaluates the security, privacy, and dependability parameters along with the scales defined for what the range of values represents.

A detailed analysis and working of the European SHIELD approach as proposed by Noll et al. [9] is explained in the next section. It is to be noted that multimetrics approach of Noll et al. relies on the weight values of the component and subcomponent of a system from the expert in a given field of their expertise [9]. As different experts may have a different opinion on choosing the different weight values of the component and subcomponent of a system, a consensus cannot be reached using Noll et al. approach.

Therefore, this paper proposes to harness the collective advantage of *Human Swarming* known as *Artificial Swarm Intelligence (ASI)* in the real-time closed-loop system where each human member of a group can participate forming a unified swarm like birds or fishes and reach the consensus in evaluating the weight values of different components and subcomponents of the automated vehicles system. We have studied three use case scenarios to evaluate our approach in accessing the *security*, *privacy*, and *dependability* of such automated vehicles.

The rest of the paper is organized as follows. In Section 2, we describe the model for automated vehicles with vehicular fog computing. This section also deals with the security and privacy issues of automated vehicles in such vehicular environment. Multimetrics approach of Noll et al. [9] is explained in Section 3. Our *crowd-based intelligence* approach which is inspired from *swarm intelligence* for accessing the *security*, *privacy*, and *dependability* metrics for automated vehicles is explained in Section 4. In Section 5, we discuss three use case scenarios representing *security*, *privacy*, and *dependability* issues in automated vehicles. In Section 6, we evaluate our approach. Finally, conclusion and future works of our paper are drawn in Section 7.

## 2. Internet of Automated Vehicles with Vehicular Fog Computing

Automated vehicles use a lot of sensors, GPS, and roadside units (RSU) such as video cameras to sense its surrounding environment. They also use the radio system for effective communication, control area network bus sensors to monitor its internal operation status, and cloud computing for large and heavy computation, data analysis and visualization for optimization and storage, and so on. However, it should be noted that there is a latency in processing the data and computing it in the cloud [10]. To cope up with the

emergency situations, we need to reduce the *latency* in data computation. Otherwise, the result will be potentially disastrous considering the number of automated vehicles at a certain place on the roads at a certain time. Taking the advantage of information-centric networking (ICN) and named data networking (NDN), we also need to think of the quality of services (QoS) of the users of automated vehicles who wants to access the content of their choice such as multimedia service and applications on the fly in real-time without any *delay* and *jitter*. *Fog computing* can help to act in emergency situations by reducing latency and improving QoS. It is a new paradigm of bringing cloud services to the edge of the automated vehicles network. In the case of automated vehicles, a vehicular fog can be formed by sharing the resources of a number of automated vehicles and roadside units such as video cameras at a certain place at a certain time [11].

Figure 1 shows the Internet of automated vehicles with vehicular fog computing concept where the vehicular fog is formed by utilizing the combined computing resources of automated vehicles ( $AV_1, AV_2, AV_3, AV_4$ , and  $AV_5$ ) and roadside units ( $RSU_1$  and  $RSU_2$ ). Automated vehicles ( $AV_1$ ) broadcast the association request, and nearby automated vehicles  $AV_2, AV_3, AV_4$ , and  $AV_5$  and roadside units  $RSU_1$  and  $RSU_2$  respond to the request of  $AV_1$  forming a common vehicular fog which each of the automated vehicles can use it for the effective operation. The vehicular fog could be formed by the association of several automated vehicles, and roadside units may change depending on the need of automated vehicles; that is, if  $AV_5$  wants to leave the group, then it will broadcast dissociation request, and the other automated vehicles respond by acknowledging it and allowing  $AV_5$  to leave the group. Now, the same process of broadcasting the association request by a particular automated vehicle follows to form a new vehicular fog with active participation from nearby vehicles and roadside units. The sensors such as temperature and humidity sensors which are supporting the applications of automated vehicles also send their respective sensing data to the vehicular fog for local processing at the edge, which can be used by different automated vehicle's users and their applications in the network. Furthermore, the contents and information browsed by different automated vehicles and locally cached in the vehicular fog will reduce the latency and increase the QoS of such automated vehicles and users. Also, the data are sent from the vehicular fog to the cloud for different purposes such as data mining, large and heavy computation, analysis, optimization, and long time storage. Based on the work of Hou et al. [12] and Kai et al. [13], a comprehensive difference between cloud and fog computing is shown in Table 1. Also, our use case scenario "Real-time data processing in vehicular fog" as explained later in Section 5.1 clearly explains the benefits of having fog computing paradigm in an automated vehicular environment. Although we have different advantages of cloud and vehicular fog for the smooth operation, interconnecting several automatic vehicles together brings its own set of security, privacy, and dependability issues. We will discuss in detail about security and privacy issues of

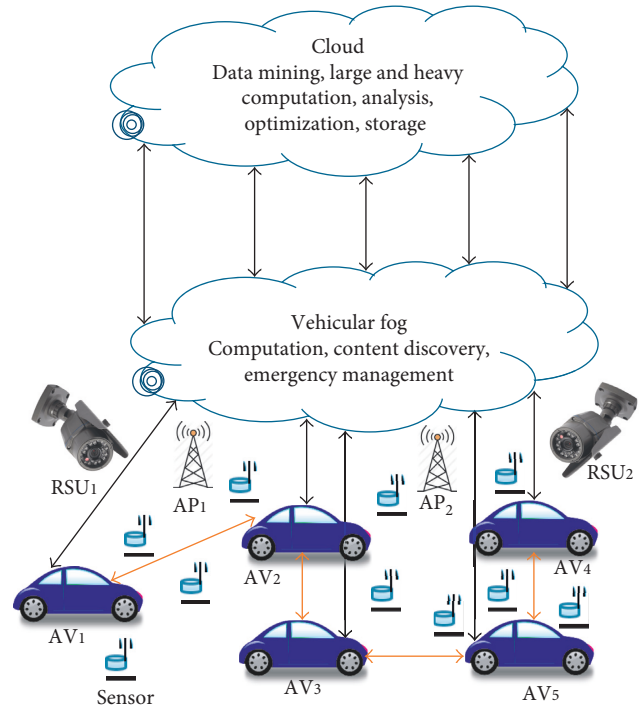


FIGURE 1: Internet of automated vehicles with vehicular fog computing.

automated vehicles in the next subsection. We will also discuss different case scenarios of automated vehicles considering security, privacy, and dependability issues in the next section.

**2.1. Security and Privacy Issues in Internet of Automated Vehicles.** Due to smart sensing and proliferation of IoT technologies, each of our automated vehicles will be equipped with hundreds of sensors supporting various applications for its successful operation and making our lives much easier for smart mobility. The work by Parkinson et al. has surveyed a large volume of publicly accessible literature on connected and automated vehicles and argued that with all connected computing infrastructures and the rise of the level of computational functionality and connectivity increases the exposure of potential vulnerabilities, which can further increase the likelihood of future attacks [14]. Saxena et al. have discussed the security and privacy challenges and requirements for smart vehicle-to-grid (V2G) networks [15]. They have also proposed an architecture to tackle anonymous authentication, access control, information confidentiality, message integrity, and so on. The work by Amoozadeh et al. have explained the effects and consequences of security attacks on a communication channel of a connected vehicle stream [16]. It also deals with security attacks such as sensor tampering of a connected vehicle stream to achieve cooperative adaptive cruise control (CACC).

When our automated vehicles get connected to the Internet and if an attacker has access to it, he can fully

TABLE 1: Cloud computing versus fog computing.

Requirement	Cloud computing	Fog computing
Latency	High	Low
Delay jitter	High	Very low
Location of server nodes	Within the Internet	At the edge of the local network
Distance between the client and server	Multiple hops	One hop
Security	Undefined	Can be defined
Attack on data en-route	High probability	Very low probability
Location awareness	No	Yes
Geographical distribution	Centralized	Distributed
Support for mobility	Limited	Supported
Target users	General Internet users	Mobile users
Connectivity	Communicate through IP networks	Wireless interface
Bandwidth requirements	Sensitive for bandwidth	Less demand for bandwidth

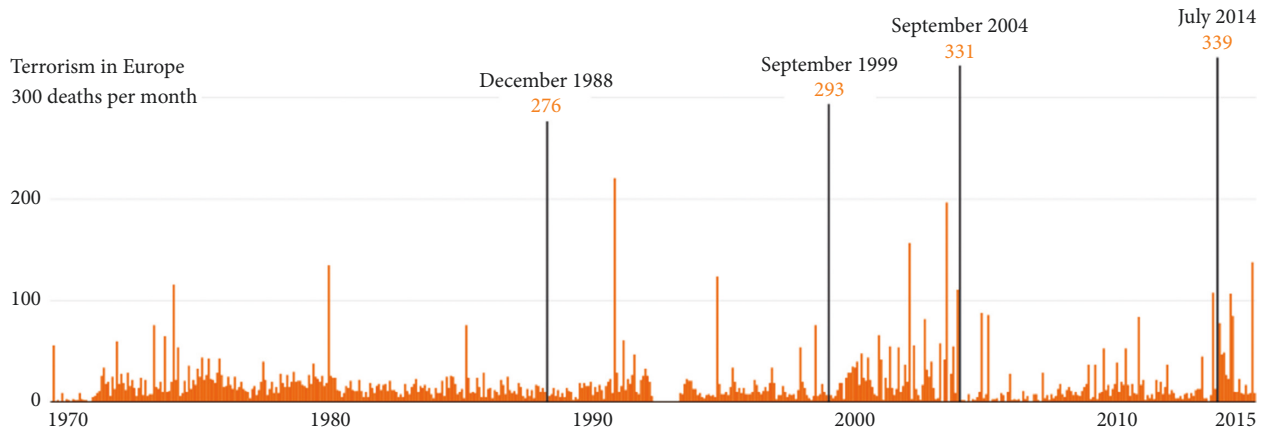


FIGURE 2: Terrorism in Europe [18].

exercise control over our vehicle and can perform *ransomware* attacks. *Ransomware* attacks are the new types of attacks, and it is growing day by day as more number of smart things are getting connected to the Internet providing more opportunities for the hackers to hack our system [17]. Imagine a situation that a hacker gains access to our automated vehicle and he/she can also easily access our *push/pull* data traffic. Hacker may demand the user of the automated vehicle to transfer a certain amount of cryptocurrency or bitcoin to his personal account. On denying to accept the proposal of the attacker, he may increase the inside temperature of an automated vehicle or may not open the door of the vehicle. Also, the attackers can make the automated vehicle to collide with other nearby vehicles. As a user, we can do nothing in such situations but have to accept to the term of the proposal of the *ransomware* attacker. The security issue with our automatic vehicles could be even worse when our vehicles are being used for terrorism without our knowledge or consent.

Figure 2 shows a survey data about terrorism in Europe from 1970 to 2015 [18]. We can see the number of terrorist attacks and fatalities in Europe. Moreover, the number of

vehicle ramming attacks has also increased at an alarming rate costing the lives of thousands of people. We have comprehensively outlined the number of vehicle ramming attacks, especially in Europe from 2002 to 2017 as it is shown in Table 2. Imagine a situation, where terrorists can remotely hack into our automated vehicles sitting at certain parts of the world to perform vehicle ramming attacks. This would be a national security issue of any country. As a user enjoying the benefits of automated vehicles for smart mobility, we also need to consider the security of our automated vehicles seriously. Furthermore, it should be noted that an automated vehicle may use the data of other sensors equipped on other automated vehicles for its operation such as visualizing traffic or accessing content *locally cached on the vehicular fog*. So, breaching the security of one automated vehicle could result in the security breach of other vehicles and so on.

While there are benefits of the fully automatic and connected cars, they also raise up privacy issues. Privacy issues include, what if somebody hacked the personal data of the user traveling in such automated vehicles or things or person seen by the equipped video camera on the vehicle to other vehicle users. What if our vehicles are

TABLE 2: Vehicular ramming attacks in Europe.

Country	Year	Number of fatalities	Reasons of the attack
Lyon, France	2002	0 (the building was empty)	Attacks on Jewish targets
Scotland, Glasgow	2007	1 death and 5 nonfatal injuries	Islamism-inspired ramming attack
Netherlands	2009	8 deaths and 10 nonfatal injuries	Vehicular attack
London, UK	2013	1 death and 2 nonfatal injuries	Islamic terrorism attack
Dijon, France	2014	0 death and 11, nonfatal injuries	Islamism-inspired ramming attack
Nantes, France	2014	1 death and 10 nonfatal injuries	Suspected mental unbalance
Iserre, France	2015	1 death and 2 nonfatal injuries	Vehicle ramming terrorism
Graz, Austria	2015	3 deaths and 36 nonfatal injuries	Vehicular attack terrorism
Nice, France	2016	87 deaths and 434 nonfatal injuries	Vehicular attack and shooting
Berlin, Germany	2016	12 deaths and 56 nonfatal injuries	Islamism-inspired ramming attack
Westminster, UK	2017	5 deaths and 50 nonfatal injuries	Islamic terrorism attack
Antwerp, Belgium	2017	0 death and 0 nonfatal injuries	Terrorism attack
Stockholm, Sweden	2017	4 deaths	Terrorism attack

continuously being tracked and anyone can know the current location of us through our vehicle tracking. This would result in privacy violation for the users of such automated vehicles for smart mobility. Thus, privacy is equally an important issue in the context of the Internet of automated vehicles.

### 3. Multimetrics Approach

The SHIELD multimetrics (MM) as proposed by Noll et al. [9] can be applied to evaluate *security*, *privacy*, and *dependability* of a system. The MM approach works by

- (1) dividing the system into smaller logical components called subsystems;
- (2) defining the suitable metric for each subsystem;
- (3) calculating the security, privacy, and dependability score (denoted as triplet of  $(S, P, D)$ ) of the entire system;
- (4) comparing the security, privacy, and dependability score of the entire system with the required application goal of the system to find the best configuration of the system.

The MM approach by Noll et al. [9] is shown in Figure 3. The SPD system is composed of individual *security*, *privacy*, and *dependability* levels defined by  $(S, P, D)$  where each element is represented by a value in the range of 0 to 100. This means, the higher the range, the stronger the security, privacy, and dependability levels. The MM approach is based on two parameters: the actual criticality  $(c_{i(S)}, c_{i(P)}, c_{i(D)})$  of each component of the subsystem and the weight  $(w_{i(S)}, w_{i(P)}, w_{i(D)})$  and  $(W_{i(S)}, W_{i(P)}, W_{i(D)})$  is the weight values (between 0 and 100) of each component of the subsystem. Criticality is a triplet defined as the complement of  $(S, P, D)$  and expressed as  $(C_S, C_P, C_D) = (100, 100, 100) - (S, P, D)$ .

The criticality  $(C_{i(S)}, C_{i(P)}, C_{i(D)})$  is calculated by the root mean square weighted data (RMSWD) formula:

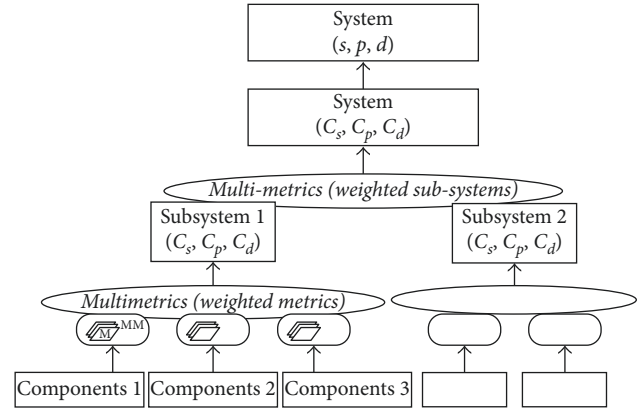


FIGURE 3: Multimetrics approach as proposed by Noll et al. [9].

$$C_{i(S)} = \sqrt{\frac{c_{i(S)}^2 * w_{i(S)}}{\sum_i w_{i(S)}}}$$

$$C_{i(P)} = \sqrt{\frac{c_{i(P)}^2 * w_{i(P)}}{\sum_i w_{i(P)}}} \quad (1)$$

$$C_{i(D)} = \sqrt{\frac{c_{i(D)}^2 * w_{i(D)}}{\sum_i w_{i(D)}}},$$

$$w_{i(S)} = \left(\frac{W_{i(S)}}{100}\right)^2$$

$$w_{i(P)} = \left(\frac{W_{i(P)}}{100}\right)^2 \quad (2)$$

$$w_{i(D)} = \left(\frac{W_{i(D)}}{100}\right)^2,$$

$$(S_i, P_i, D_i) = (100, 100, 100) - (C_{i(S)}, C_{i(P)}, C_{i(D)}). \quad (3)$$

Since 100 is the maximum scale we set it for security, privacy, and dependability, the lower the criticality of the components, the higher is the security of the component as shown by (3). Now, the best configuration of the system is chosen by comparing the predefined goal values of the system with the closest result obtained from (3). The MM approach has certain limitations, and this model relies on the *expert opinion* on choosing the weight values for each of the components which is *highly subjective* as a different expert may give different grading scheme based on their level of expertise in the field. Different values of weight for the components from the experts will lead to different results. Thus, the obtained results are not comparable.

In order to make the MM approach generally applicable, consensus need to be reached. Therefore, a concrete and closed system model is required where we can trust the evaluation of the system. This motivates us to apply the *crowd-based intelligence* approach [19] that is inspired by *swarm intelligence* as an improvement to the MM approach in evaluating the security, privacy, and dependability in automated vehicles.

#### 4. Crowd-Based Intelligence Approach Inspired by Swarm Intelligence: A UNU Artificial Swarm Intelligence Approach

Scientific research has shown that a group can perform better than individuals in making decisions and predictions [19]. This is known as collective intelligence of the group or crowd where the decision is entirely contributed by the whole group of members. We have particularly seen the intelligence in the fish swarming and bird flocking where they form a closed-loop system that converges to solutions in synchrony. As a human being, we did not evolve the ability to form swarms and flocks as fishes and birds do. It is because of the lack of innate connection to establish continuous feedback loops as other species do for making collective decisions from their group members. Thus, we need some sort of similar mechanism to perform human swarming in the closed-loop system to harness the collective intelligence.

Inspired by the natural bio-inspired algorithms, Rosenberg et al. have proposed an UNU platform to harness the collective advantage of *Human Swarming* known as *Artificial Swarm Intelligence (ASI)* in the real-time closed-loop system where each human member of a group can participate forming a unified swarm like birds or fishes and reach the consensus [19]. UNU is an online real-time platform where users can log in from anywhere around the world forming a closed loop of swarming process [20]. As shown in Figure 4, given a scenario, we asked different experts for choosing the optimum value of the  $S, P, D$  values on the UNU online platform to form a closed loop and come up with the best values for  $(S, P, D)$  values for a particular scenario where security is the major concern for automated vehicles. The optimum value as chosen by different experts forming a swarm in the closed-loop process on the UNU ASI platform converges to  $(S, P, D) = (90, 60, 45)$  which is

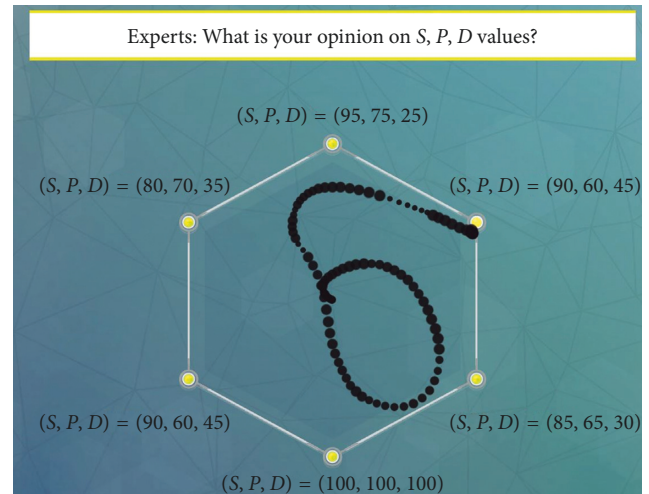


FIGURE 4: Crowd-based intelligence approach inspired by Swarm Intelligence: A UNU Artificial Swarm Intelligence approach.

clearly shown in Figure 4. For detail working of the online UNU platform and approach, kindly refer to the paper [19]. Throughout this paper, for all of our evaluation of the scenarios on the UNU ASI platform, experts refer to the group of researchers ( $> 3$ ) at the University of Oslo, Norway who have a good knowledge in security and applicability to IoT.

#### 5. Use Case Scenarios for Automated Vehicles: An Evaluation of Security, Privacy, and Dependability

To evaluate the *security*, *privacy*, and *dependability* metrics of automated vehicles, we have used three use case scenarios of automated vehicles. The three use cases are derived from Figure 1, which is further decomposed into *system*, *sub-system*, and *component* level as shown in Figure 5. We will discuss each of these use cases in detail.

**5.1. Real-Time Data Processing in Vehicular Fog.** We have already explained the need and formation of vehicular fog from the active participation of a number of collaborating automated vehicles and roadside units to form a common resource pool which they can use it for real-time data processing. We need to process data in real-time to take necessary actions to ensure safety of the automated vehicular user. In such situations, an automated vehicle might want to notify the nearby hospital about the accident and call the ambulance along with the location of the accident so that the help can be sought in near real-time. It would also be necessary to inform the police and family members about the accident. Moreover, other automated vehicles might not see the road blocked by the accident and may crash at the same place. So, it is also necessary to notify other traffic flowing through the same road where the accident has occurred. Other automated vehicles also need to be notified about the accident for their safety. Automated vehicles might also want other nearby vehicles and people to help overcome

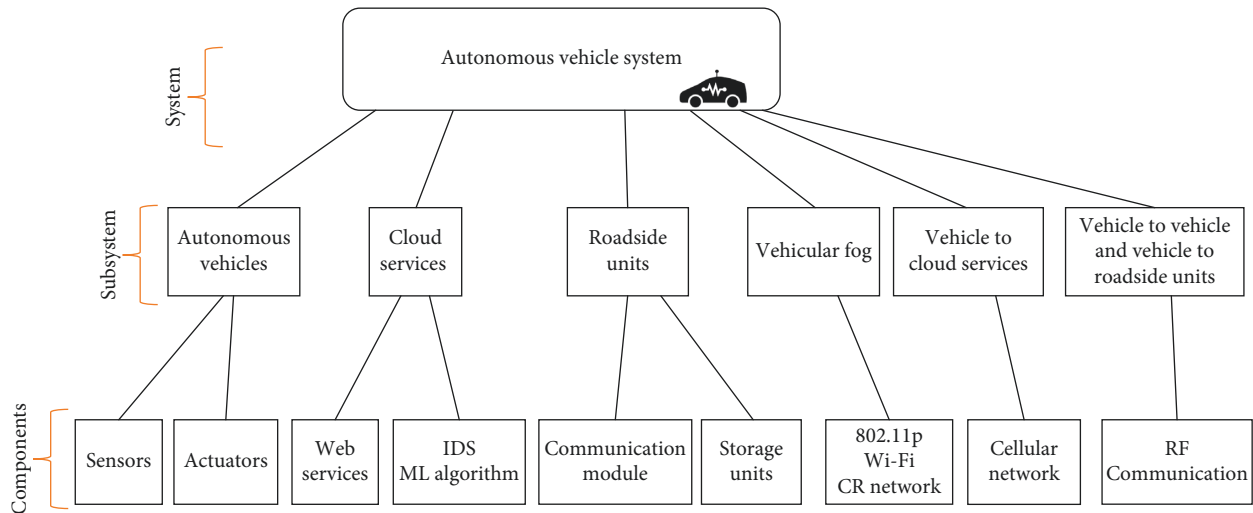


FIGURE 5: System-, subsystem-, and component-level break down of automated vehicle system.

these emergency situations. All these information and data should be processed in real-time near to the automated vehicles and this is where the advantage of vehicular fog comes into play.

So as to reduce the latency in such critical situations, we argue that real-time data processing in vehicular fog is the best solution. Furthermore, automated vehicles might want this critical notification to reach respective destination guaranteed. So, communication is the backbone for the automated vehicular environment. Without communication, we cannot imagine the automated vehicles running on the roads. Let us say, if a message can not be sent due to a weak cellular network, it should be possible to send it through any available underlying network until it reaches the intended destination. Here, we also propose the use of cognitive radio (CR) technology to take the advantage of selecting the available channel for communication. Also, there might be roadside units such as video cameras which can help in sending such messages in the case of delivery failure. That means the accident notification must be quite reliable and dependable. This clearly shows the dependability context of automated vehicles on vehicular fog and communication channel. Furthermore, it should also be noted that automated vehicles can communicate with each other and roadside units using *802.11p* protocol. In other nonemergency situations and processing of data in the cloud without worrying about time constraint, automated vehicles can make use of usual GSM (2G/3G or above) communication. In addition to this, as we are taking advantage of the vehicular fog, the communication must be single hop so as to reduce the latency. The configuration of these parameters is subject to the situation, the latency requirements, the severity of the requested service, or application, and it needs to be processed for every given situation in mind.

**5.2. Secured Communication of Data in Vehicular Fog and Cloud.** Secured communication in the automated vehicular environment either in vehicular fog or cloud is a potential

approach to mitigate the number of attacks on automated vehicles.

Such automated vehicles that are connected to the Internet without any human inputs will be an easy target for the terrorists to carry out their motive. Take, for example, automated vehicles fully depend on image processing sensors and units to map real-world 3D environment of the road ahead and surrounding environments and make decisions on the fly. For instance, if a hacker is able to compromise our automated vehicles and starts sending out the spoofed image to the processing unit in the vehicular fog or cloud, as the input is wrong, automated vehicles will produce the wrong result which we do not want in any case. Here, comes the role of machine learning (or deep learning) and intrusion detection algorithms to efficiently tackle secured communication of data in the vehicular fog and the cloud. The communication of automated vehicle data in the vehicular fog and the cloud can be supported through radio link *802.11p* protocol, using cognitive radio (*802.11/802.15.4*) technologies [21, 22] with encrypted data validated and authorized by the smart vehicle owner either in the vehicular fog or the cloud.

**5.3. Value-Added Services in Automated Vehicles.** With the development of automated vehicles and technologies, there would be a change from vehicle provision to service provision for automated vehicular users. Users can enjoy the multimedia services without any delay and jitter. Thanks to the NDN and ICN architecture which the automated vehicle user can use it in the vehicular fog and cloud with an improved QoS. Users can also opt for online shopping and banking on the fly. Or even more, automated vehicles can provide other value-added services such as measuring all the vital signs of a person. There will be a wide variety of sensors equipped inside the automated vehicles measuring our heart condition, blood pressure, pulses, and so on and notify a family member or hospital if any unusual health condition is detected. These services are some of the luxury services

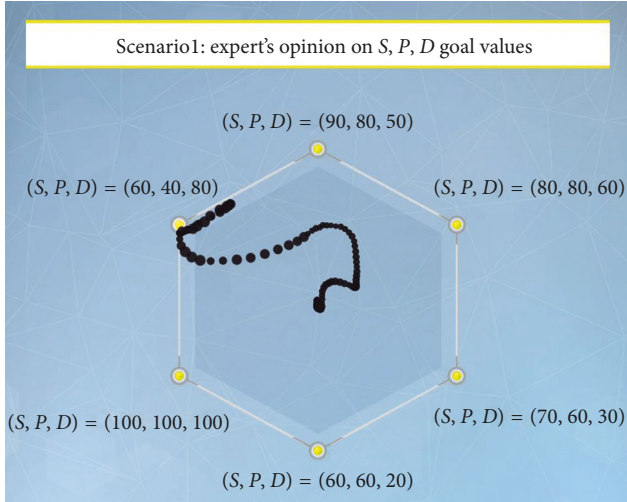


FIGURE 6:  $(S, P, D)_{\text{Goal}}$  values for scenario 1: real-time data processing in vehicular fog on the UNU ASI platform.

which we, as a smart automated vehicle's user, can use it anytime and anywhere during our travel. However, privacy and confidentiality of the data traffic generated by the automated vehicles should be maintained by the system. If there is any privacy violation of the user in such sensitive data related to location, banking, health details, and multimedia services are exposed, users may not want to use such luxury services and even automated vehicles. Such private and sensitive data can be used by the hackers to expose the details of the user to the unfavorable scenarios that a user do not want in any case and can be even used for ransomware attacks.

## 6. Evaluation through Crowd-Based Intelligence Approach for Accessing Security, Privacy, and Dependability of Automated Vehicles

For our three use case scenarios, we asked the group of experts to form a closed group on the UNU ASI platform for their opinion on  $S, P, D$  goal values. The consensus of the experts for  $S, P, D$  goal values for our three use cases on the UNU ASI platform are shown in Figures 6–8, respectively. The  $S, P, D$  goal values for the three use cases is shown in Table 3. Similarly, the subsystem weight as shown in Table 4 and  $S, P, D$  criticality weight  $(C_s, C_p, C_d)$  of the component for different configurations and different component weight as shown in Table 5 is calculated by the experts on the UNU ASI platform for all the three use cases. The different metrics used to measure  $S, P, D$  level is also shown in Table 5. After we calculated the criticality of all the components as shown in Tables 6–8, respectively, we have several  $(S, P, D)$  values based on our configurations. We have 24 possible configurations as shown in Tables 6–8 for our three use cases that we could use to compute our  $S, P, D$  metrics. As the automated vehicular system is divided into several independent subsystems, we select the appropriate configuration which suggests the closest values to the  $(S, P, D)$  goal that has

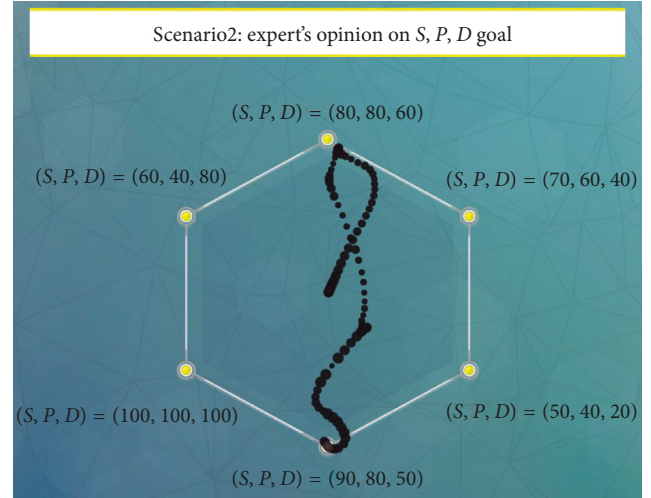


FIGURE 7:  $(S, P, D)_{\text{Goal}}$  values for scenario 2: secured communication of data in vehicular fog and cloud on the UNU ASI platform.

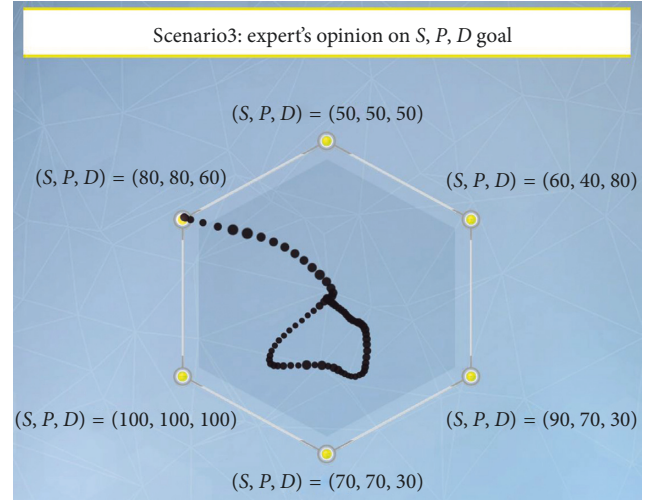


FIGURE 8:  $(S, P, D)_{\text{Goal}}$  values for scenario 3: value-added services in automated vehicles on the UNU ASI platform.

been set out in Table 3. Besides, only one subsystem is responsible to handle a scenario that we have considered. Therefore, several values that we got were easily converging towards the subsystems and up to the system without exploding into several new configurations. From Table 6, we can see the security criticality calculation for our 3 use cases with different configurations and subsystems and the security level of the configuration that matches our security goal has been selected. Similarly, from Table 7, we can see the privacy criticality calculation for our 3 use cases with different configurations and subsystems and the privacy level of the configuration that matches our privacy goal has been selected. Finally, from Table 8, we can see the dependability criticality calculation for our 3 use cases with different configurations and subsystems and the dependability level of the configuration that matches our dependability goal has been selected.



TABLE 3: SPD<sub>Goal</sub> of use cases.

Use case	Security	Privacy	Dependability	SPD <sub>Goal</sub>
Real-time data processing in vehicular fog	60	40	80	(60, 40, 80)
Secured communication of vehicles and data in vehicular fog/cloud	90	80	50	(90, 80, 50)
Value-added services in automated vehicles	80	80	60	(80, 80, 60)

TABLE 4: Weights of the subsystem.

Subsystem	Weight ( $W_i$ )
Vehicular fog	70
Radio link	70
Mobile link	50

TABLE 5: Component, component weight, and configurations.

Subsystem	Component	Component weight	Configurations	$C_s$	$C_p$	$C_d$
Vehicular fog	Radio link	70	With encryption	30	30	10
			Without encryption	70	80	30
	GSM (2G/3G or above)	50	2G	70	80	60
			3G or above	50	40	40
	802.11p	60	With encryption	20	30	40
			Without encryption	80	80	60
With authentication			10	20	20	
Without authentication			90	70	70	
Radio link	Cognitive radio	70	With encryption	30	30	40
			Without encryption	70	80	60
			With authentication	30	20	20
			Without authentication	80	70	70
Mobile link	Access control	60	Enabled	30	20	30
			Disabled	90	60	70
	Encryption	70	ON	30	30	30
			OFF	70	80	70

*Scenario 1* was about the safety and accident reporting and system responsible for handling such situations, and therefore it needs to be *highly dependable*. However, privacy can be compromised in this scenario as well. Therefore, we set the ( $S, P, D$ ) goal of (60, 40, 80) as suggested by the experts on the *UNU ASI* platform. The best configuration that we got, when encryption was enabled and when the mobile network was above 2G with the ( $S, P, D$ ) value (62, 60, 72) which is reasonably acceptable. We get a higher value in privacy though it was not of much importance in this scenario. This is because when the dependability needs to have higher importance, there must be some level of security which is strong enough to securely send the messages to the desired target.

Similarly, *scenario 2* was about secured communication in the fog and cloud which focused more on security and privacy with ( $S, P, D$ ) goal of (90, 80, 50). The closest value we could obtain was (76, 80, 80) when the authentication of both *cognitive radio* and *802.11p* was enabled. We got higher dependability values because dependability is coupled with security and privacy.

*Scenario 3* was about entertainment and value-added services that can be provided via autonomous vehicles.

Obviously, privacy and security requirement should be higher in this case. The best configuration obtained for this scenario was (70, 74, 70) against an ( $S, P, D$ ) goal of (80, 80, 60). It was obtained when both the access control and encryption were enabled.

The final selected configuration  $S, P, D$  level for each of our use case is shown in Table 9. The colour representation in Table 9 is selected according to the numeric difference between SPD level and SPD<sub>Goal</sub>, using the following criteria that we have set out:

- (i)  $|\text{SPD}_{\text{Goal}} - \text{SPD level}| = <10$ , green ●
- (ii)  $|\text{SPD}_{\text{Goal}} - \text{SPD level}| = >10, <20$ , yellow ●
- (iii)  $|\text{SPD}_{\text{Goal}} - \text{SPD level}| = >20$ , red ●

where the green circle represents perfectly matching case between SPD<sub>Goal</sub> and actual SPD calculated during the evaluation of different configurations of the use case scenarios. Similarly, the yellow and red circles represent good and bad match case between SPD<sub>Goal</sub> and actual SPD calculation, respectively.

The advantage of our framework is that by selecting the subsystem and configurations properly, the assessment of the security, privacy, and dependability parameters

TABLE 6: Calculation table for security criticality for selected configuration.

Cs1	Cs2	Component weight_w1	Significance weight_w1	Component weight_w2	Significance weight_w2	Total significance weight ( $\Sigma$ )	Final configuration criticality	Security level	Configuration	Subsystem	Selected configuration
30	70	70	0.49	50	0.25	0.74	47	53	Configuration1		
30	50	70	0.49	50	0.25	0.74	38	62	<b>Configuration2</b>	Vehicular fog	<b>Selected for scenario 1</b>
70	70	70	0.49	50	0.25	0.74	70	30	Configuration3		
70	50	70	0.49	50	0.25	0.74	64	36	Configuration4		
20	30	60	0.36	70	0.49	0.85	26	74	Configuration1		
20	70	60	0.36	70	0.49	0.85	55	45	Configuration2		
20	30	60	0.36	70	0.49	0.85	26	74	Configuration3		
20	80	60	0.36	70	0.49	0.85	62	38	Configuration4		
80	30	60	0.36	70	0.49	0.85	57	43	Configuration5		
80	70	60	0.36	70	0.49	0.85	74	26	Configuration6		
80	30	60	0.36	70	0.49	0.85	57	43	Configuration7		
80	80	60	0.36	70	0.49	0.85	80	20	Configuration8		
10	30	60	0.36	70	0.49	0.85	24	76	Configuration9	Radio link	
10	70	60	0.36	70	0.49	0.85	54	46	Configuration10		
10	30	60	0.36	70	0.49	0.85	24	76	<b>Configuration11</b>		<b>Selected for scenario 2</b>
10	80	60	0.36	70	0.49	0.85	61	39	Configuration12		
90	30	60	0.36	70	0.49	0.85	63	37	Configuration13		
90	70	60	0.36	70	0.49	0.85	79	21	Configuration14		
90	30	60	0.36	70	0.49	0.85	63	37	Configuration15		
90	80	60	0.36	70	0.49	0.85	84	16	Configuration16		
30	30	60	0.36	70	0.49	0.85	30	70	<b>Configuration1</b>		<b>Selected for scenario 3</b>
30	70	60	0.36	70	0.49	0.85	57	43	Configuration2	Mobile link	
90	30	60	0.36	70	0.49	0.85	63	37	Configuration3		
90	70	60	0.36	70	0.49	0.85	79	21	Configuration4		




TABLE 7: Calculation table for privacy criticality for selected configuration.

Cp1	Cp2	Component weight_w1	Significance weight_w1	Component weight_w2	Significance weight_w2	Total significance weight ( $\Sigma$ )	Final configuration criticality	Privacy level	Configuration	Subsystem	Selected configuration
40	80	70	0.49	50	0.25	0.74	57	43	Configuration1		
40	40	70	0.49	50	0.25	0.74	40	60	<b>Configuration2</b>	Vehicular fog	<b>Selected for scenario 1</b>
80	80	70	0.49	50	0.25	0.74	80	20	Configuration3		
80	40	70	0.49	50	0.25	0.74	69	31	Configuration4		
30	30	60	0.36	70	0.49	0.85	30	70	Configuration1		
30	80	60	0.36	70	0.49	0.85	64	36	Configuration2		
30	20	60	0.36	70	0.49	0.85	25	75	Configuration3		
30	70	60	0.36	70	0.49	0.85	57	43	Configuration4		
80	30	60	0.36	70	0.49	0.85	57	43	Configuration5		
80	80	60	0.36	70	0.49	0.85	80	20	Configuration6		
80	20	60	0.36	70	0.49	0.85	54	46	Configuration7		
80	70	60	0.36	70	0.49	0.85	74	26	Configuration8		
20	30	60	0.36	70	0.49	0.85	26	74	Configuration9	Radio link	
20	80	60	0.36	70	0.49	0.85	62	38	Configuration10		
20	20	60	0.36	70	0.49	0.85	20	80	<b>Configuration11</b>		<b>Selected for scenario 2</b>
20	70	60	0.36	70	0.49	0.85	55	45	Configuration12		
70	30	60	0.36	70	0.49	0.85	51	49	Configuration13		
70	80	60	0.36	70	0.49	0.85	76	24	Configuration14		
70	20	60	0.36	70	0.49	0.85	48	52	Configuration15		
70	70	60	0.36	70	0.49	0.85	70	30	Configuration16		
20	30	60	0.36	70	0.49	0.85	26	74	<b>Configuration1</b>		<b>Selected for scenario 3</b>
20	80	60	0.36	70	0.49	0.85	62	38	Configuration2	Mobile link	
60	30	60	0.36	70	0.49	0.85	45	55	Configuration3		
60	80	60	0.36	70	0.49	0.85	72	28	Configuration4		

TABLE 8: Calculation table for dependability criticality for selected configuration.

Cd1	Cd2	Component weight_w1	Significance weight_w1	Component weight_w2	Significance weight_w2	Total significance weight ( $\Sigma$ )	Final configuration criticality	Dependability level	Configuration	Subsystem	Selected configuration
20	60	70	0.49	50	0.25	0.74	38	62	Configuration1		
20	40	70	0.49	50	0.25	0.74	28	72	<b>Configuration2</b>	Vehicular fog	<b>Selected for scenario 1</b>
50	60	70	0.49	50	0.25	0.74	54	46	Configuration3		
50	40	70	0.49	50	0.25	0.74	47	53	Configuration4		
40	40	60	0.36	70	0.49	0.85	40	60	Configuration1		
40	60	60	0.36	70	0.49	0.85	52	48	Configuration2		
40	20	60	0.36	70	0.49	0.85	30	70	Configuration3		
40	70	60	0.36	70	0.49	0.85	59	41	Configuration4		
60	40	60	0.36	70	0.49	0.85	49	51	Configuration5		
60	60	60	0.36	70	0.49	0.85	60	40	Configuration6		
60	20	60	0.36	70	0.49	0.85	42	58	Configuration7		
60	70	60	0.36	70	0.49	0.85	66	34	Configuration8		
20	40	60	0.36	70	0.49	0.85	33	67	Configuration9	Radio link	
20	60	60	0.36	70	0.49	0.85	47	53	Configuration10		
20	20	60	0.36	70	0.49	0.85	20	80	<b>Configuration11</b>		<b>Selected for scenario 2</b>
20	70	60	0.36	70	0.49	0.85	55	45	Configuration12		
70	40	60	0.36	70	0.49	0.85	55	45	Configuration13		
70	60	60	0.36	70	0.49	0.85	64	36	Configuration14		
70	20	60	0.36	70	0.49	0.85	48	52	Configuration15		
70	70	60	0.36	70	0.49	0.85	70	30	Configuration16		
30	30	60	0.36	70	0.49	0.85	30	70	<b>Configuration1</b>		<b>Selected for scenario 3</b>
30	70	60	0.36	70	0.49	0.85	57	43	Configuration2	Mobile link	
70	30	60	0.36	70	0.49	0.85	51	49	Configuration3		
70	70	60	0.36	70	0.49	0.85	70	30	Configuration4		

TABLE 9: Selected configuration SPD level for each use case.

Use case	SPD <sub>Goal</sub>	Configuration	Actual SPD	SPD <sub>Goal</sub> versus Actual SPD
Real-time data processing in vehicular fog	(60, 40, 80)	Encryption and mobile network above 2G	(62, 60, 72)	
Secured communication of vehicles and data in vehicular fog/cloud	(90, 80, 50)	Authentication in both IEEE, 802.11p, and cognitive radio	(76, 80, 80)	
Value-added service in automated vehicles	(80, 80, 60)	Access control and encryption enabled	(70, 74, 70)	

converges for several configurations allowing us to select the appropriate configuration of a system based on a simple comparison.

## 7. Conclusion and Future Works

With the proliferation of device-to-device (D2D), machine-to-machine (M2M), and the Internet of things (IoT) technologies, automated vehicles have created a new wave of revolution in automobile industries. However, in order to fully establish automated vehicles and their connectivity to the surroundings, security, privacy, and dependability always remain a crucial issue. Therefore, prior analysis of different attack trends and vulnerabilities in such automated vehicles is essential in order to deploy proactive and security solutions effectively. Systematic approaches to measure efficient system configuration, security, privacy, and dependability of such systems are essential for getting the overall picture of the system such as design patterns and best practices for configuration of a system. Decomposing a system into components and subsystems, a multimetrics (MM) methodology developed through European SHIELD project is an early evaluation approach allowing easy accessibility of the security, privacy, and dependability components to choose the suitable configuration of a system.

However, MM methodology completely relies on the values of weights of different components chosen by an expert that is highly subjective based on their level of expertise in the field. Different values of weight of the components from the experts will lead to an unjustified and unreliable result. Thus, an agreement on standardization of weight is one of the major challenges.

Therefore, we proposed a crowd-based intelligence approach that is inspired by a swarm intelligence forming a closed-loop system like swarms in humans as groups can perform better in analyzing and reaching the consensus. We evaluated three use case scenarios of automated vehicles and systems with vehicular fog. We finally have evaluated the security, privacy, and dependability metrics with different configurations for our automated vehicles with vehicular fog computing scenario in choosing the best configuration for our system.

The best configuration for *scenario 1* with SPD<sub>Goal</sub> values of **(60, 40, 80)**, the calculated *S, P, D* values through our method closest to the SPD<sub>Goal</sub> with best configuration was found out to be **(62, 60, 72)**. Similarly, the best configuration for *scenario 2* with SPD<sub>Goal</sub> values of **(90, 80, 50)**, the calculated *S, P, D* values through our method closest to the

SPD<sub>Goal</sub> with best configuration was found out to be **(76, 80, 80)**. Finally, the best configuration for *scenario 3* with SPD<sub>Goal</sub> values of **(80, 80, 60)**, the calculated *S, P, D* values through our method closest to the SPD<sub>Goal</sub> with best configuration was found out to be **(70, 74, 70)** as summarized in Table 9.

For future work, we will use this crowd-based intelligence approach in evaluating other IoT system and propose efficient solutions to counteract security and privacy issues of such systems.

## Conflicts of Interest

The authors declare no conflicts of interest.

## Acknowledgments

The authors would like to thank Josef Noll for his valuable feedback on the applicability of the multimetrics approach given our novel assessment of weightings of components. The authors would also like to thank György Kálmán for providing valuable insight into measurable security topics in IoT which were very helpful in writing this paper.

## References

- [1] C.-W. Tsai, C.-F. Lai, and A. V. Vasilakos, "Future internet of things: open issues and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2201–2217, 2014.
- [2] U. Krishnamurthy and P. P. Maglio, "Paves: partnering with autonomous vehicles, environments, and systems," in *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 003 381–003 386, Budapest, Hungary, October 2016.
- [3] T. ElBatt, C. Saraydar, M. Ames, and T. Talty, "Potential for intra-vehicle wireless automotive sensor networks," in *Proceedings of the IEEE Sarnoff Symposium*, pp. 1–4, Princeton, NJ, USA, March 2006.
- [4] C. D. Harper, C. T. Hendrickson, S. Mangones, and C. Samaras, "Estimating potential increases in travel with autonomous vehicles for the non-driving, elderly and people with travel-restrictive medical conditions," *Transportation Research Part C: Emerging Technologies*, vol. 72, pp. 1–9, 2016.
- [5] S. Muralidharan, B. Sahu, N. Saxena, and A. Roy, "PPT: a push pull traffic algorithm to improve QoS provisioning in IoT-NDN environment," *IEEE Communications Letters*, vol. 21, no. 6, pp. 1417–1420, 2017.
- [6] T. Bécsi, S. Aradi, and P. Gáspár, "Security issues and vulnerabilities in connected car systems," in *Proceedings of the 2015 IEEE International Conference on Models and*

- Technologies for Intelligent Transportation Systems (MT-ITS)*, pp. 477–482, Budapest, Hungary, June 2015.
- [7] K. Koscher, A. Czeskis, F. Roesner et al., “Experimental security analysis of a modern automobile,” in *Proceedings of the 2010 IEEE Symposium on Security and Privacy (SP)*, pp. 447–462, Oakland, CA, USA, May 2010.
  - [8] M. Steger, M. Karner, J. Hillebrand, W. Rom, and K. Römer, “A security metric for structured security analysis of cyber-physical systems supporting SAE J3061,” in *Proceedings of the IEEE 2016 2nd International Workshop on Modelling, Analysis, and Control of Complex CPS (CPS Data)*, pp. 1–6, Vienna, Austria, April 2016.
  - [9] J. Noll, I. Garitano, S. Fayyad et al., “Measurable security, privacy and dependability in smart grids,” *Journal of Cyber Security and Mobility*, vol. 3, no. 4, pp. 371–398, 2014.
  - [10] A. Rauniar, P. Engelstad, B. Feng et al., “Crowdsourcing-based disaster management using fog computing in internet of things paradigm,” in *Proceedings of the 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, pp. 490–494, Pittsburgh, PA, USA, November 2016.
  - [11] E.-K. Lee, M. Gerla, G. Pau, U. Lee, and J.-H. Lim, “Internet of vehicles: from intelligent grid to autonomous cars and vehicular fogs,” *International Journal of Distributed Sensor Networks*, vol. 12, no. 9, pp. 1–14, 2016.
  - [12] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, and S. Chen, “Vehicular fog computing: a viewpoint of vehicles as the infrastructures,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 6, pp. 3860–3873, 2016.
  - [13] K. Kai, W. Cong, and L. Tao, “Fog computing for vehicular ad-hoc networks: paradigms, scenarios, and issues,” *Journal of China Universities of Posts and Telecommunications*, vol. 23, no. 2, pp. 56–96, 2016.
  - [14] S. Parkinson, P. Ward, K. Wilson, and J. Miller, “Cyber threats facing autonomous and connected vehicles: future challenges,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 11, pp. 2898–2915, 2017.
  - [15] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, “Network security and privacy challenges in smart vehicle-to-grid,” *IEEE Wireless Communications*, vol. 24, no. 4, pp. 88–98, 2017.
  - [16] M. Amoozadeh, A. Raghuramu, C.-N. Chuah et al., “Security vulnerabilities of connected vehicle streams and their impact on cooperative driving,” *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, 2015.
  - [17] T. Ring, “Connected cars—the next target for hackers,” *Network Security*, vol. 2015, no. 11, pp. 11–16, 2015.
  - [18] C. Alcantara, “45 years of terrorist attacks in Europe, visualized,” 2017, <https://www.washingtonpost.com/graphics/world/a-history-of-terrorism-in-europe>.
  - [19] L. Rosenberg, D. Baltaxe, and N. Pescetelli, “Crowds vs swarms, a comparison of intelligence,” in *Proceedings of the Swarm/Human Blended Intelligence Workshop (SHBI) (IEEE)*, pp. 1–4, Cleveland, OH, USA, October 2016.
  - [20] “Unu beta, think together,” 2017, <http://unu.ai/>.
  - [21] A. Rauniar, D. R. Jeong, G. K. Chand, and S. Y. Shin, “Performance analysis of cascaded energy and matched filter detector with malicious users in cognitive radio networks,” in *Proceedings of the 2015 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, pp. 629–633, Nusa Dua, Bali, Indonesia, November 2015.
  - [22] A. Daniel, A. Paul, A. Ahmad, and S. Rho, “Cooperative intelligence of vehicles for intelligent transportation systems (ITS),” *Wireless Personal Communications*, vol. 87, no. 2, pp. 461–484, 2016.

