RICAV: RIsk based Context-Aware Security Solution for the Intra-Electric Vehicle Network

Yosra Fraiji[1,2], Lamia ben Azzouz[1], Wassim Trojet[2], Ghaleb Hoblos[2] and Leila Azouz Saidane[1]
[1]*RAMSIS Team, CRISTAL Laboratory, National School of Computer Science, 2010 Campus University, Manouba, Tunisia*
[2]*Normandie Univ., UNIROUEN, ESIGELEC, IRSEEM, 76000 Rouen, France*

Keywords: Context-Aware Security Solution, Risk, Intra-Vehicle Network, Electric Vehicle, Game Theory.

Abstract: Smart electric vehicles are equipped with many ECU (Electronic Control Unit) that provide high levels of safety and comfort to the drivers. However, the intra-vehicle networks are targeted by hackers as they are of great interest both in terms of processing power (botnets) and in terms of economic value (ransomware). Therefore, static security solutions were proposed, both by researchers and car manufacturers, to secure the Intra-Electric Vehicle Sensors network (IVSN). However, these solutions are energy-intensive and could deplete the battery along the travel, affecting the driver safety.For this purpose, we aim to propose an adaptive security solution, called RIsk-based Context-Aware security solution for the intra-Vehicle network (RICAV), that considers the electric vehicle context (energy, distance to the charging stations, traffic state, etc) and the risk assessment value to provide a trade-off between security and energy consumption. Simulation experiments were conducted to evaluate the proposed approach in terms of robustness and energy consumption.

1 INTRODUCTION

Electric vehicles have taken a great attention from government and car manufacturers in order to improve environment wellbeing. However, the adoption of wireless technologies for the intra-vehicle communication has raised more security concerns. Many attacks can be performed on the intra-vehicle network such as eavesdropping, spoofing, DoS, etc (Reinhard et al., 2020). Authors in (Nie, Liu, and Du 2017; Pan et al., 2017) showed, the way to hack the car functions such as the engine management software, door locking and starting system). To avoid cyber-attacks on the intra electric vehicle network, existing security solutions implement the most robust security mechanisms (Corbett et al., 2018). In (Fraiji et al., 2019), authors showed that according to the cryptographic algorithm (AES, 3DES, etc) implemented, the energy consumption could increase by about 15% of the battery capacity. Existing connected vehicles security solutions were designed for carbon cars and use permanently the most robust security mechanisms. For EV, that could deplete the battery along the travel and could affect the driver safety. Hence, static solutions are not suitable for the electric vehicle ecosystem. Therefore, (Fraiji et al., 2019), authors proposed a Context-Aware SecurIty solution for the Electric Vehicle (CASIEV) that provides a trade-off between security and energy consumption. In this solution, the context of the vehicle (energy, distance to the charging station, traffic, etc) is considered, when the battery level is critical, to secure the system as long as possible along the route.

In another hand, the risk is defined as Threat likelihood × Impact (NIST, 2012). The likelihood estimates the attack feasibility (probability of success). The Impact (also called severity) indicates the assessment of the risk level and intensity. Many works (ETSI, 2017), (Kaveh Bakhsh Kelarestaghi, Mahsa Foruhandeh, Kevin Heaslip, 2019), (Shaikh and Thayananthan, 2019), in the literature, investigated the risk assessment. Furth-ermore, some works designed security solutions based on the risk (Arfaoui et al., 2018; Gebrie and Abie 2017; Pham, Makhoul, and Saadi, 2011), (Atlam et al., 2020). Indeed, the authors propose approaches adapting the level of security to network intrusion risk value.

The main concern in this work is to combine the context used in CASIEV (focusing mainly on enhancing the energy delivery process) with the risk assessment of an intrusion into the intra-EV network in order to improve real-time decision on the relevant

Fraiji, Y., ben Azzouz, L., Trojet, W., Hoblos, G. and Saidane, L.
RICAV: RIsk based Context-Aware Security Solution for the Intra-Electric Vehicle Network.
DOI: 10.5220/0010581407720778
In *Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT 2021)*, pages 772-778
ISBN: 978-989-758-524-1

security level activation. The new approach we called RICAV RIsk-based Context-Aware security solution for the intra-Vehicle network improves CASIEV by extending more the lifetime of the security system. Indeed, according to RICAV, there is no need for a high level of security when the risk is low, even if there are no energy constraints. However, according to CASIEV if there are no energy constraints, the security level must be high. RICAV is modelled using game theory considering two players (energy management system and security system) as game theory is suitable for modelling systems with conflicting objectives in order to find the trade-off between them. The rest of this paper is organized as follows: Section 2 presents a risk assessment background. Section 3 describes the RICAV system. Simulation results are discussed in Section 4. A brief conclusion addresses the contributions and perspectives of this work.

2 RISK ASSESSMENT BACKGROUND

In the literature, the risk assessment has attracted the attention of researchers and standardization bodies that issued several standards. The NIST (USA National Institute of Standards and Technology) risk assessment (NIST, 2012) includes system characterization, threat sources and events, system vulnerabilities identification, security countermeasures evaluation and risk determination (impact-likelihood matrix). Therefore, it detects, evaluates and prioritizes risks. The ETSI TVRA (Threat, Vulnerability and Risk Analysis) study the risk in the context of the vehicular network. It identifies risks, their likelihood and impact. Furthermore, it involves seven steps: identify security objectives and security requirements, produce an inventory of system assets, classify system vulnerabilities and threats, quantify the likelihood and impact of attacks, determine the risks involved and specify detailed security requirements. The SecRAM (Marotta et al., 2013) method is the ISO 27005 based risk assessment management methodology that was developed for air traffic management. It associates a value between 1 and 5 to the threat impact on the security services (Availability (Av), Authentication (Au), Confidentiality (C), Integrity (I) and Non-repudiation (Nr)). Furthermore, it considers the highest impact service (Av, Au, C, I and Nr) as an overall threat impact. Many works in the literature investigated risk assessment in the context of the in-vehicle network. In (Kaveh Bakhsh Kelarestaghi, Mahsa Foruhandeh, Kevin Heaslip, 2019), authors adapted (NIST, 2012) in the context of a compromised in-vehicle network. The goal of this methodology is to explore threats targeting the in-vehicle networks and to map impacts of such threats into risk clusters. For example, they consider safety and behavioural impacts as a very high risk. In (Shaikh and Thayananthan, 2019) authors proposed a fuzzy risk-based decision for vehicular networks while adopting the NIST risk definition at a high level. However, they use new mechanisms to identify the likelihood and impact value. The likelihood is based on the vehicle context (lane, road, traffic, weather, speed and time) and the driver's attitude. On the other hand, the impact is calculated based on the type of application. The EVITA project(Ruddle and Ward, 2009) (Esafety Vehicle Intrusion Protected Applications) proposed an intra-vehicle risk assessment. It is considered as a prominent risk assessment model that adopted the asset-oriented approach. EVITA proposed a risk matrix that includes attacks likelihood, the attack severity, and the driver controllability. The severity is calculated in terms of four factors: Safety, privacy of drivers, operational performance, and financial losses. The likelihood of a threat is considered in terms of the expertise, knowledge of target, window of opportunity (including time requirement).

3 RISK-BASED CONTEXT-AWARE SECURITY SOLUTION FOR THE INTRA-VEHICLE NETWORK

The Intra-Vehicle Network is a complex network of sensors, ECUs and firmware that can be vulnerable to many types of attacks. Our goal is to minimize the energy consumption of the system while maintaining the security of the Intra-Vehicle Network communications as long as possible along the route.

3.1 RICAV Architecture

Figure 1 presents the architecture of RICAV. It is composed of two systems: CASIEV (Context-Aware Security for the Intra-Electric Vehicle) (Fraiji et al., 2019) and ASR (Adaptive Security based on the Risk). CASIEV adapts the security of the in-vehicle sensors network according to the EV dynamic context. We defined the context as the State of Charge (SoC), the nearest available charging station, the sensor resources (memory and processing) and the

traffic conditions. CASIEV applies the high security level allowed by the context without considering the risk probability. The ASR module chooses the required security level according to the risk in order to improve the energy saving process. If the risk is low, there is no need to ask for a high security level which is an energy incentive.

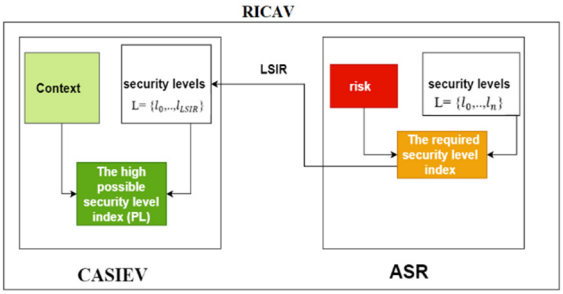

Figure 1: RICAV architecture.

3.2 Which Modelling Approach for RICAV?

In this work, we face a multi-objective optimization problem as it requires more than one objective function to be optimized simultaneously (preserving security and optimizing energy).In the literature, many techniques are used to solve this problem such as Weighted-sum method, e-constraints Method, Multi-level Programming, Goal Programming, Evolutionary Algorithm (Genetic Algorithm, Differential Evolution) and game theory. In (Sfar et al., 2019), authors showed that game theory outperforms many well-known multi-objective and meta-heuristic algorithms in quality, stability, convergence speed, and running time.Game theory balances the trade-off between conflicting objectives (Liang and Xiao, 2013).Furthermore, it is adapted to this case study as it can model scenarios in which there is no centralized entity with a full picture of network conditions.Indeed, the security system does not have any information about the battery SoC (State of Charge) and vice versa.

Game theory is used in network security as a quantitative framework which studies the interaction between hackers and defenders(Liang and Xiao, 2013). In fact, many authors adopted the Game theoretic approach to model adaptive security solutions. In (Hamdi and Abie, 2014), authors proposed a game theoretical model for an e-Health adaptive security preserving the authentication of smart things. Authors provided a mathematical model, relying on Markov game theory, to present healthcare under dynamic context. This model, based on a set of strategies to design the game model, uses four basic parameters to represent the context (memory, communication channel, energy depletion model and the threat model). In (Xiaolin et al. 2008), authors developed an adaptive security model relying on Markov chain for the network information system. This work is based on two Markov chains. The first chain was used to model the propagation of both the threats in the network and the quantified risk. The second one adapted the security of the system according to the quantified risk.

3.3 Game based Risk and Context-Aware Security Formulation

RICAV (RIsk based Context Aware Security for the intra-Vehicle network) is a game-based risk and context aware solution. In the considered scenario, players compete for the limited network resources (in our case: energy). In this section, we will present the parameters, assumptions, game specification, game tree, Nash equilibrium and the behavioural System Model.

3.3.1 Assumptions

We assume that:

- The proposed game is a Non-Cooperative Dynamic Game Incomplete Information in which two players compete with each other. A non-cooperative game is one in which any cooperation must be self-enforcing, as players are strictly rational and play to optimize their individual expected value. The game is dynamic as we consider a dynamic vehicular context (dynamic energetic context and risk). In the complete game all players have the same privileges and knowledge about the game conditions and the other players' strategies and actions.In the incomplete information players don't have the information of the other players, however it needs to identify other players choices and hence predict its behaviour.
- The game is a sequential game in which players alternate turns. The security system will play its strategy and the energy system will in turn react.

3.3.2 Game Specification

The game G is defined as a triplet (P, S, U), where P is the set of players, S is the set of strategies, and U is the set of payoff functions (Manshaei et al., 2013). In the proposed strategy, we consider two players: the energy management system and the security system.

The energy management system represents the key player of the game. For each player we will describe their strategies, utility function and pay-offs. The security system adapts the security level of sensors according to the identified risk. The energy management system aims to optimize the energy consumption of the intra-electric vehicle network according to the context. In this section, we begin by describing the game of player 1. Then, we will describe the game of player 2.

Players: P= {security system (ss), energy management system (es)}.

Stage 1: Security System Player.

Let L= $\{l_0, l_1,..,l_n\}$ be the set of security levelsL_i, 0 ≤ i ≤ n

S_{ss} is the set of strategy of the security system

$$S_{ss} = L$$

Utility of the player 1:maximizing the robustness of the security system while minimizing the overhead (processing, memory, delay). The robustness of a network will be assessed as the degree of the security strategy capability to withstand attacks. The security system adapts the security level (l) according to the risk value r .

U_{ss} represent the Pay-offs of the security system.

$$U_{ss} = G(p_l)$$

The Payoff Function is modelled by a sigmoid function, as demonstrated in (Sfar et al., 2019).The sigmoid value is between [0, 1]. This function is classified as a nonlinear, quickly increasing and simple function which can meet the requirement of calculating the required security level probability in a reasonable running time.

the gain function G ($\boldsymbol{p_l}$)is defined as in (1)

$$\mathbf{G}(\boldsymbol{p_l}) = \frac{1}{1+e^{-g_l*(p_l-h_l)}}, \boldsymbol{g_l = r, \forall\, r > 0.05} \qquad (1)$$

with g_l the steepness of sigmoid function, h_l: the center of the sigmoid function. In practice,$g_l$represents the risk level. We consider the r=0 as a special case. The equation $\frac{1}{1+e^{-g_l*(p_l-h_l)}}$ cannot reflect the reality as for all probabilities value the function will return always 0.5. For this purpose, if risk (r) is equal to zerog_l =10 (2). p_l is the probability of using the required security level l_i .

$$\mathbf{G}(\boldsymbol{p_l}) = \frac{1}{1+e^{-g_l*(p_l)}}, \boldsymbol{r = 0.05, g_l = 10} \qquad (2)$$

Stage 2: Energy Management System Player.

Let E= {on , off},

S_{es} be the set of strategy of Energy management system player.S_{es}= E

The energy management system is in the on mode if it accepts to deliver the required energy and in the off mode otherwise.

Utility Function of the Player 2: The energy management system provides the good operation of the intra-vehicle network with a minimal cost (minimizing the energy consumption).

U_{es} represent the Pay-offs of the energy management system (3). U_{es}= L (p_e)

$$\mathbf{L}(\boldsymbol{p_e}) = \frac{1}{1+e^{-g_e*(p_e-h_e)}} \qquad (3)$$

with g_e: the steepness of sigmoid function,h_e: the center of the sigmoid function. In practice, the g_e reflect the system state. It is equal to 0.05 if the system is green, 0.5 if the system is orange, 1 if the system is red (see table 1). p_e is the probability of delivering the required energy.

Table 1: Energy management system state.

System state	Description
Green state ($g_e = 0.05$)	The energy management system accepts to deliver energy.
Orange state ($g_e = 0.5$)	The energy management system can accept or refuse to deliver energy. This decision is based on the context parameters (charging station and traffic).
Red state ($g_e = 1$)	The energy management system refuses to deliver energy.

Stage 3: General Objective Function.

The two parameters p_l and p_e probabilities are defined independently. However, in the present model the only context in which the security system adapts the required security strategy is when it has the required energy. We can conclude that the two events are the same and their probabilities coincide. For this purpose, we can define $p_{lr} := p_l = p_e$. The objective of the game is to maximize the function (4). It is continuous and defined on a compact, which is easy to prove in our case.

$$\mathbf{U}(\mathbf{p_{lr}}) = (\mathbf{G}(\mathbf{p_{lr}}) * (\mathbf{1} - \mathbf{L}(\mathbf{p_{lr}}))) \qquad (4)$$

3.3.3 Equilibrium Solution

The utility functions defined above express a trade-off between (energy and security):

- Enforcing the policy (at the risk of depleting the battery)

- Using a less robust security level (at the risk of violating the security policy).

The equilibrium of the game is denoted by (eq^*) and is found by solving the following optimization problem (5).

$$\mathbf{eq: = argmax\ \{U\ (p_{lr}), p_{lr}\ \in [0..1]\ \}} \quad (5)$$

eq is the value of p_{lr} maximizing the utility function and thereby, reflecting the optimal probability of disclosing the required security level. In the particular case, we can retrieve the optimum value of eq explicitly $g_e = g_l$ and $h_l > h_e$. In the general case, the value of eq is calculated numerically (see the simulation section).

4 SIMULATION AND ANALYSIS

We solve the game equilibrium for different situations in the game numerically. We represent the gain function **G (p_l)** and the loss function **L (p_e)**, calculate their product, find their maximum point and get the corresponding steady state. To simulate different scenarios, we modify the g_l and g_e values (risk and energy level) and analyse the player's behaviour. Figures 2, 3 and 4 present results for a scenario where the energy is available (g_e=0.005 green energetic state and the risk value varies. We notice in the figures 2,3,4 a Nash equilibrium. Indeed, both players are winners as the energy is available, hence giving the energy may not result in an important loss (the loss will always be moderate). Figure 2 shows that the gain of the security system (robustness) is very low if the probability of obtaining the required security level is low and it can reach 1 in the opposite case. In such scenario, the RICAV prioritize the security then the energy consumption.

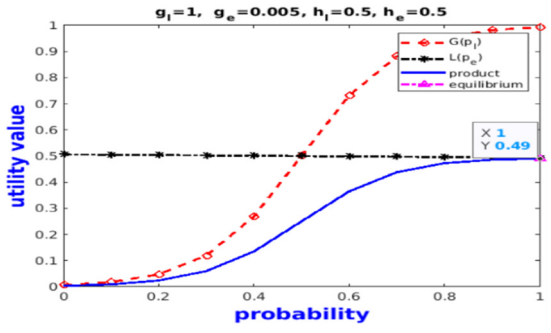

Figure 2: Nash equilibrium for risk=1 and green energetic state.

In figure 3, since the risk is equal to 0.5, the gain of the security system is more important than in the previous case even for a low probability.

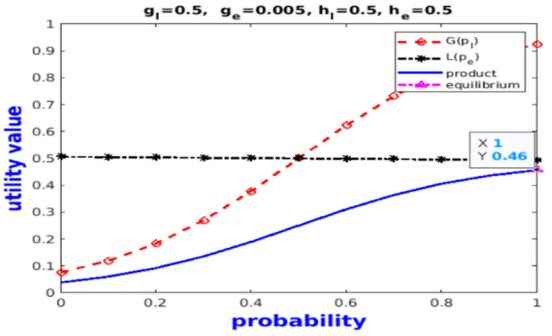

Figure 3: Nash equilibrium for risk=0.5 and green energetic state.

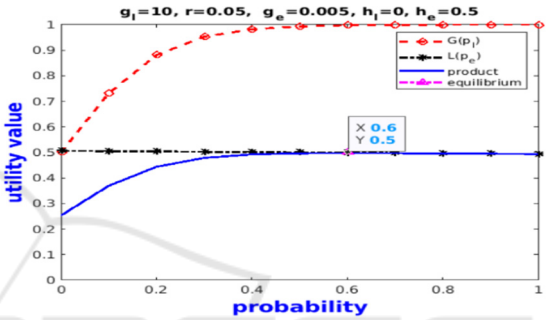

Figure 4: Nash equilibrium for risk= 0.05 and green energetic state.

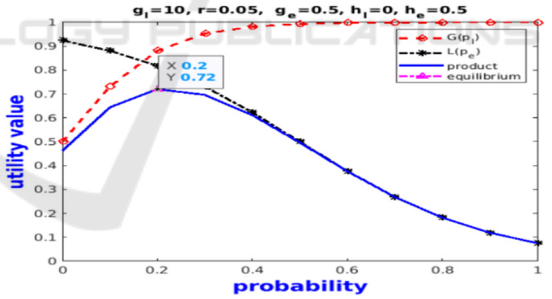

Figure 5: Nash equilibrium for risk=0.05 and orange energetic state.

In figure 4, we have considered a risk equal to 0.05. We notice that the robustness of the system is high even if the security level is not provided since the risk of attack is almost inexistent. Indeed, the decrease in risk leads to an increase in the robustness of the system. In this case, RICAV can ask for a low security level (or no security at all) even though the energy is available. Figure 5 present results for a scenario where the energy has become critical (g_e=0.5 orange energetic state) and the risk value varies. In this case, we obtain a Nash equilibrium only in the case where the risk is very low (r=0.05). Indeed,

since the battery can deliver or does not deliver energy, there is always a winner and a loser. In this scenario, RICAV provides a trade-off between energy and security. It prioritizes security if the risk is high and prioritizes energy saving if the risk is low. In the red energetic state, we consider a battery in the red zone where the energy becomes very critical. In this case, we obtain a Nash equilibrium only in the case where the risk is very low (r=0.05) since the energy system is not allowed to supply energy in this zone. That means, the equilibrium probability when the risk is low (r=0.05) is not related to the decision of the energy management system. In this scenario RICAV prioritizes energy saving.

5 CONCLUSION

In this work, we proposed a risk-based context-aware security solution for the intra-electric vehicle sensor network. This solution allows the system to preserve energy as it adapts the security according to the risk and the vehicular context (energy, distance to charging station, traffic, etc). RICAV is modelled using game theory. The game is composed of two players: the security system and the energy management system. The security system adapts the security level according to the identified intrusion risk. The energy management system provides the energy amount required by the security system according to the vehicle context. Simulations show that the robustness of the system grows when the risk decreases. Therefore, RICAV prioritizes the energy saving process if the risk is low. It prioritizes security if the energy is available and the risk is high or medium. For future works, we intend to improve RICAV by developing a trust model for the intra-EV network intrusion risk assessment based on the vehicle current context and its previous experience. Indeed, considering the risk trust value could enhance the energy saving process. For example: if the risk is high and the trust is low, the system can ask for a low security level improving this way the energy saving process.

REFERENCES

Arfaoui, Amel, Ali Kribeche, Sidi Mohammed Senouci, and Mohamed Hamdi. 2018. “Game-Based Adaptive Risk Management in Wireless Body Area Networks.” In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, IEEE, 1087–93.

Atlam, Hany F. et al. 2020. “Risk-Based Access Control Model: A Systematic Literature Review.” *Future Internet* 12(6): 1–23.

Corbett, Christopher et al. 2018. “Leveraging Hardware Security to Secure Connected Vehicles.” *SAE Technical Paper Series* 1: 1–12.

ETSI. 2017. “Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA).” 1: 1–88.

Fraiji, Yosra et al. 2019. “Adaptive Security for the Intra-Electric Vehicular Wireless Networks.” *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*: 1215–20.

Gebrie, Mattias T, and Habtamu Abie. 2017. “Risk-Based Adaptive Authentication for Internet of Things in Smart Home EHealth.” In *Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings*, , 102–8.

Hamdi, Mohamed, and Habtamu Abie. 2014. “Game-Based Adaptive Security in the Internet of Things for EHealth.” *2014 IEEE International Conference on Communications, ICC 2014*: 920–25.

Kaveh Bakhsh Kelarestaghi, Mahsa Foruhandeh, Kevin Heaslip, Ryan Gerdes. 2019. “Intelligent Transportation System Security : Networks.”

Liang, Xiannuan, and Yang Xiao. 2013. “Game Theory for Network Security.” *IEEE Communications Surveys & Tutorials* 15(1): 472–86.

Manshaei, Mohammad Hossein et al. 2013. 45 ACM Computing Surveys *Game Theory Meets Network Security and Privacy*.

Marotta, Antonio et al. 2013. “Applying the SecRAM Methodology in a CLOUD-Based ATM Environment.” *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013* (December): 807–13.

Nie, Sen, Ling Liu, and Yuefeng Du. 2017. “Free-Fall: Hacking Tesla from Wireless to Can Bus.” *Defcon*: 1–16.

NIST. 2012. “NIST Special Publication 800-30 Revision 1 - Guide for Conducting Risk Assessments.” *NIST Special Publication* (September): 95.

Pan, L et al. 2017. “Journal of Information Security and Applications Cyber Security Attacks to Modern Vehicular Systems.” *Journal of Information Security and Applications* 36: 90–100.

Pham, Congduc, Abdallah Makhoul, and Rachid Saadi. 2011. “Risk-Based Adaptive Scheduling in Randomly Deployed Video Sensor Networks for Critical Surveillance Applications.” *Journal of Network and Computer Applications* 34(2): 783–95.

Reinhard, Jan Peter, Marcel Kneib, Martin Ring, and Oleg Schell. 2020. “Assessment of Current Intrusion Detection System Concepts for Intra-Vehicle Communication.” : 1–2.

Ruddle, Alastair, and David Ward. 2009. “Security Requirements for Automotive On-Board Networks Based on Dark-Side Scenarios.” (1): 138.

Sfar, Arbia Riahi, Yacine Challal, Pascal Moyal, and Enrico Natalizio. 2019. “A Game Theoretic Approach for

Privacy Preserving Model in IoT-Based Transportation." *IEEE Transactions on Intelligent Transportation Systems* PP: 1–10.

Shaikh, Riaz Ahmed, and Vijey Thayananthan. 2019. "Risk-Based Decision Methods for Vehicular Networks." *Electronics (Switzerland)* 8(6).

Xiaolin, Cui, Tan Xiaobin, Zhang Yong, and Xi Hongsheng. 2008. "A Markov Game Theory-Based Risk Assessment Model for Network Information System." *2008 International Conference on Computer Science and Software Engineering*: 1057–61.