Rapid Establishment of Transient Trust for NDN-Based Vehicular Networks

Sanjeev Kaushik Ramani
Florida International University
skaus004@fiu.edu

Alex Afanasyev
Florida International University
aa@cs.fiu.edu

***Abstract*—Recent advances of vehicular networking technologies are giving birth to the emerging class of road safety and collaborative driving applications, where cars need to communicate and assist each other with various tasks, such as sharing views from onboard cameras, performing distributed predictions of car positions, etc. The proposed Named Data Networking (NDN) architecture promises a straightforward way to implement such applications with enhanced data delivery and security capabilities. However, one of the critical elements of vehicular applications is the need of reliable trust: the communicating cars must ensure that parties will do the job they are asked to do. Such trust, while can be mechanically implemented through the use of cryptographic signatures, requires the establishment of trust relations between the cars. This is especially a challenge, given the individual cars in a typical urban environment can very infrequently meet each other and each encounter could be very short-term. Although one can rely on a manufacturer-centric endorsement of car actions (e.g., by installing manufacturer certificates as global trust anchors, creating manufacturer-signed certs for individual cars, and trusting data that is signed by such certificates), it is not sufficient for the collaborative applications. Such certificate can only tell that data is coming from the specific car model, but does not guarantee the quality of the data/actions. This paper considers ideas and concepts developed based on the Swift Trust model and explores their use in vehicular environments with NDN-based communication. With Swift Trust, vehicles in the communication range can quickly make short-term trust decisions for secure publishing, consumption, and processing of data (e.g., to cooperatively analyze the nearby environment for potential safety issues). As an initial step, the paper explores a task-oriented method of establishing trust based on request-response communication. The paper also highlights several potential threats and attacks and discusses possible directions to mitigate them.**

I. Introduction

Trust plays an integral part in network communications. It effectively determines from whom and from which services or applications, users accept information or are willing to send information. Trust can broadly be categorized under *static/knowledge-based* or *dynamic/interaction-based* trust. The static/knowledge-based trust expects the communicating entities to possess complete or partial knowledge about the other entity, e.g., gained based on prior encounters or from trusted third parties. Dynamic/interaction-based trust involves entities willing to collaborate on a common task without any prior interactions or the involvement of trusted third parties.

In traditional approaches to trust establishment, the communicating parties can rely on pre-existing configurations—pre-configured sets of root Certification Authority (CA) certificates and transitive trust in Public Key Infrastructure (PKI) model—or dynamically build trust relations—using feedback or explicitly setting trust decisions of certificate trustworthiness in Web-of-Trust (WoT) model. In a highly dynamic environment like vehicular networking, these traditional methods may not work. PKI and WoT usually require connectivity to infrastructure which may not be feasible to maintain due to the mobility patterns of the vehicles. The trust relationships thus defined are usually *long-standing* and not applicable to most vehicular network applications. Existing literature on VANETs [1] suggest that in 97% cases, two vehicles come in communication proximity for less than 10 seconds. In such scenarios, message dissemination by applications and services is highly time-critical and thus needs trust computation on the fly with minimum involvement of external factors.

In this paper, we explore the applicability of social trust concepts of *Swift Trust* [2] in designing a transient trust model that can be used in the rapid bootstrapping of trust among vehicles. The problems we aim to solve using this design is (a) how to trust another vehicle into performing a task without any prior interactions with it (b) how to perform a lane change maneuver with the collaborative assistance of the surrounding vehicles (c) using the asynchronous communication model of *Named Data Networking* in successfully passing messages even in the absence of infrastructure support.

The data-centric communication model with the built-in data-centric security of Named Data Networking (NDN) [3] architecture provides unique advantages for a large class of inter-vehicular communication scenarios [4]. In particular, by focusing on data, NDN provides the opportunity for the vehicles to use any of the available communication means (e.g., WiFi or Bluetooth) to transmit and receive data. The support of in-network caching enhances communications when connectivity is intermittent. Flexible naming removes the dependency on mapping systems (e.g., DNS or cloud), allowing applications to use the network in a semantically meaningful way. However, the application of NDN still requires a proper bootstrapping of trust to ensure secure production, consumption, and processing of data, which is the objective of this paper.

Our contributions are three-fold. First, this is the first attempt to use the swift trust model in computing transient trust scores in a vehicular environment. Second, we integrated the benefits of data-centric communication using NDN in

978-1-7281-7440-2/20/$31.00 ©2020 IEEE

the dissemination of important messages. Third, we defined a specific mechanism to ensure time-limited validity of the trust scores and a possible use of ledgers in cases where trust provenance is desired.

II. Driving Example

Maneuvering through traffic and lane changes are a common sight among moving vehicles. Currently, it depends completely on the decisions made by the person operating the vehicle. The decisions are made based on the traffic conditions, assessing the speeds that the surrounding vehicles are moving with, proper indications regarding the lane change and many more. The number of parameters involved in the decision making showcases the important role that the human intellect plays in this context. Even with the human operator, there is a need for a transient trust in order to act as per the indication provided by the operator of another vehicle.

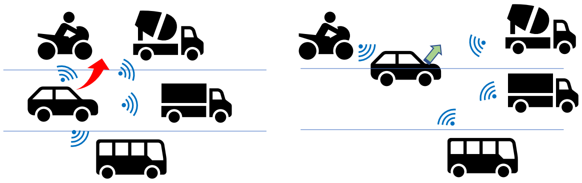

Fig. 1: Collaborative lane changes

The emerging autonomous vehicles will operate and make decisions autonomously without any human intervention, ultimately requiring multiple interactions among the vehicle to successfully perform a lane change maneuver. The onus for trust computation and usage shifts to the vehicles and these operations have to be completed in a very short duration. Any mis-communication, incorrect/insufficient processing of the requested data, or false messages in such a situation can have catastrophic effects.

To illustrate the problem and help reader's understanding of the proposed design, we will use an example shown in Figure 1: urban environment with futuristic autonomous vehicles that communicate to each other in order to achieve safe and efficient traffic movement. In our design we assume the task-oriented concepts defined in Swift trust.

III. Trust Bootstrapping

Trust bootstrapping can be defined as an onboarding process through which an entity learns the presence of other entities in the network along with learning of the other entity's current state. It is the process that prevents the infiltration of malicious nodes into the network and helps in making sure that legitimate devices or entities are getting the necessary accesses or privileges. Trust bootstrapping assists the requester in making the right choice of services [5].

Large-scale proliferation of sensors in the world and the evolution of sensors [6] have helped in automating the bootstrapping process. Bootstrapping trust in a vehicular ecosystem has significant limitations on the types of guarantees that can be offered against attacks. Section VIII introduces a few security and privacy threats.

IV. Swift Trust

The concept of Swift trust was introduced by Meyerson [7] to explain the trust paradox in temporary groups. Such groups involve individuals who did not have any prior interaction but need to collaborate to accomplish a common objective. Any temporary team has several common traits, including: (a) limited or no previous collaborations (in most cases, the entities may not work again together after the specific goal is achieved); (b) the final goal requires entities with varied skill sets (i.e., is usually very complex to achieve individually); and (c) presence of tight deadlines for meeting the goals and objectives.

Swift trust has both cognitive and normative (i.e., ideal or standard) components (Figure 2). The *cognitive components* of swift trust depends on the aggregated opinions of the communicating group about traits that are obvious. These traits could be due to the social identities the entities possess or even self-categorizations. Minimal or no prior interactions makes this component of trust computation highly critical as it leads to fostering the initial trusting behavior. The *normative components* defines a set of norms / guidelines that has to be met to enhance the early trust behaviors to be more prominent and less erosive. Setting mutually agreeable norms and meeting them improves the trusting beliefs that one entity has on the other.

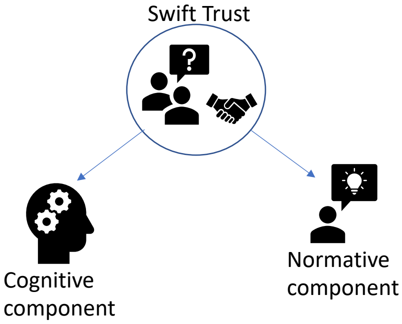

Fig. 2: Swift Trust model

Swift trust is a type of subjective trust model [7] where every node computes trust values of the neighbors/service provider based on its interaction with them. It is different from the objective model where reputation values propagate in a network and entities rely on various forms of transitive trust rules.

A. General Uses of Swift Trust

Swift trust has been extensively used and researched in the formation of global virtual teams (GVT) [7]. A GVT refers to a geographically separated team that has to work together in trying to accomplish a common goal or motive. In most cases, the team members are from entirely different backgrounds, cultures, time zones, and even expertise levels. Often, they might not have even met or had any information about how the person. However, for the objective to be achieved, all of them have to work in unison and perform their respective tasks. Swift trust establishes a temporary trust among the team members, leading to seamless collaborations. Initially, the members accept to collaborate based on the trust they possess on the project manager (the cognitive component) and the role he has in the company. Each of the members individually updates its rating or reputation values for the other member based on their performance in the task (normative component).

B. Swift Trust in NDN-Based Vehicular applications

To apply principles of Swift Trust in an car-to-car environment, we will need to realize cognitive and normative components of the safety application communication. For example, consider a lane change safety application, which involves collaborations among the cars driving on the same road, same direction, on the same and nearby lanes. The cognitive component in this case can be defined as an act of sending collaboration "signals" and collection of the corresponding responses. Such signals should be some kind of requests that can be objectively or qualitatively evaluated by the car, and can include various tasks like requesting location-aware facts about the environment (e.g., distance to nearest RSU) or various processing tasks (e.g., machine learning processing of a supplied image or video stream). After this stage, the car will be able to provide tasks to the collaborators. The tasks need to be designed so as to have responses within certain guidelines. The responses from surrounding vehicles for this task and the deviation from the defined norms will provide the normative component. The trust scores are the weighted sum of the cognitive and normative components. Once the car has recorded a trust score above a defined threshold from all the surrounding collaborators, the car will commit to doing the lane change.

The car can attempt to re-verify the integrity of the results provided by the other vehicles at any time. A random re-verification is used in times of suspicion or just to ensure that the other entity does not turn malicious after a time interval. The random nature of such re-verification confirms trust for an undisclosed period and thwarts the possibility of the collaborators turning malicious. This is based on the famous *prisoner's dilemma* concept defined in game theoretic concepts.

V. Named Data Networking

Named Data Networking (NDN) is a proposed networking architecture that uses pieces of named and secure information, data packets, as a centerpiece of communication. In other words, the NDN communication model revolves around the strategical exchange of interest and data packets. NDN defines a pull-based approach with the consumer sending an interest packet and triggering the communication [3].

The NDN architecture provides seamless support to asynchronous communication which makes it applicable for collaborative vehicular communication. The potential of in-network caches and other types of in-network storage and processing can substantially aid in designing efficient data discovery and dissemination. Moreover, each communicated data packet is cryptographically signed [8] by the producer, and thus the data is secure irrespective of where it is cached and the mode of transmission.

A specialized forwarding strategy along with the NDN data structures (Content Store (CS), Pending interest table (PIT) and Forwarding Information Base (FIB)) provides the necessary base for implementing the proposed swift trust based approach. NDN's data-centric security allows applications to control data access by using encrypted keys which are again data packets to be retrieved [3]. Having data signed and using it as the focus of communication, prevents attackers from maliciously trying to attack the devices. Immutable nature of data allows storage in multiple containers without any integrity loss and prevents producers from denying ownership of data packets.

In the case of vehicular networks, as suggested in previous works on Vehicular-NDN (V-NDN) [4], a vehicle can assume the role of either a data producer, consumer, forwarder or a data mule. Data mules are entities that participate in successful interactions and exchanges and carry the data in their CS to different locations. Data mules help in more effectively designing the forwarding strategies and the dissemination of data to remote locations thus alleviating the issues posed by intermittent connectivity. NDN's support to all these various roles provides a condition for using NDN for the exploration of the application of Swift trust. NDN fares better than IP when working in a vehicular environment as shown in [9] using a music streaming application. It is observed that NDN's stateful forwarding mechanism is highly resilient to mobility.

VI. Design Details

In the swift trust computation, the trust values are dependent on the cognitive and normative components. We consider the autonomous vehicles to have communication capacities like V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure). The Society of Automotive Engineers has defined a heartbeat Basic Safety Message (BSM) that should be communicated by each vehicle periodically. The BSM includes vehicle driving state in terms of velocity, acceleration, brake status and steering angle. On an average, the autonomous vehicles are expected to send the BSM once every 0.1 sec.

Let us also consider a road transport route to have n lanes with m segments in each lane. We assume vehicle A to be traveling in one such lane. Consider an instance of time when In any specific area in the lane (i, j) there are K vehicles. The area is defined as $1 < I < N$, $1 < j < M$. Any vehicle k in the lane can receive a message from the preceding or succeeding vehicles, say l where $(l = 1, \cdots, k-1) and 1 < k < K$.

Each communicating party, (a vehicle) assumes the role of a possible trusted entity with the desire to maintain a good reputation among other vehicles. While occupying this role, they make a promise to the requesting entity to accomplish a task at hand without any malicious intent.

As a part of this mechanism, each vehicle sends out an interest requesting the BSM data packets from its neighbors. The surrounding vehicles on receiving the interest will reply with their BSM data which will contain detials about its current state. The car that receives and aggregates these messages, can also verify them as they can compute the relative velocity, acceleration and other common surrounding parameters and compare with the received response. The proximity to the correct value will provide a higher cognitive trust score.

The car that desires to perform a lane-change maneuver will formulate some tasks based on the surroundings and the states of the vehicles it received responses from. The car also defines the guidelines for performing the tasks. The car then sends out an interest packet requesting for possible collaborators. The vehicles that are willing to collaborate and receives the interest responds with a data packet accepting a possible collaboration. The car then poses the formulated questions to the vehicle. The responses are gathered and the normative scores are computed.

The cognitive component of the trust score is computed using the following equation.

$$T_{cognitive} = (T_A + T_B + T_I)/S \tag{1}$$

where

- T_A depicts *Ability based trust* which is derived from either the sensor calculations, the manufacturers' certificate or other means that highlight the capability of the vehicle.
- T_B depicts *Benevolence based trust* which is based on how prompt and precise the responses are to the questions posed by the requester.
- T_I depicts *Integrity based trust* which is based on the manner in which the remote vehicle handles the interest messages, aggregation of the requests and responses and the prompt retransmission of the time-stamps or nonces.
- S denotes the *self-orientation* referring to the current focus of the car and what is its expectation as a response to the sent interest.

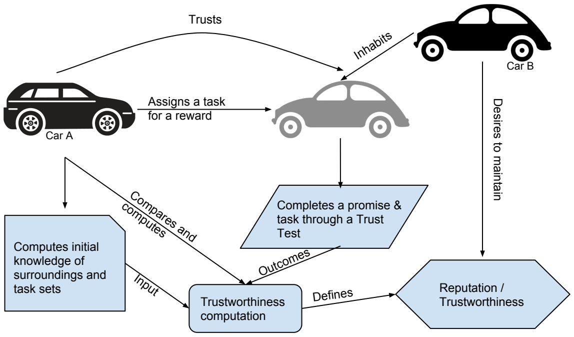
Trusts
Inhabits
Car B
Assigns a task
for a reward
Car A
Desires to maintain
Compares and computes
Completes a promise & task through a Trust Test
Computes initial knowledge of surroundings and task sets
Outcomes
Input
Defines
Trustworthiness computation
Reputation / Trustworthiness

Fig. 3: Design details

The computation of the normative component of trust involves the risk that the other vehicles is willing to take to accomplish the provided task. The performance of the task as per the set guidelines also plays an important role. The computation of the normative component is based on the game-theoretic approach involving an incentive to lure the surrounding vehicles to collaborate. A special case of *prisoner's dilema* involving a donation game is used as the approach here. According to this game, if a vehicle cooperates by performing the task, it is offering the requesting vehicle with a benefit b which is the outcome of the task at a personal computation cost c with b > c. If the vehicle declines to perform the task, it offering nothing.

If T is the temptation to perform the task, R is the reward on completion, P the punishment on not meeting the outcome and S refers to no-loss or no-gain, then based on game-theory, the collaborator will collaborate only if $T > R > P > S$. Once the vehicle is convinced to collaborate and perform the task, the responses received lead to the computation of the normative trust component and is computed using the following formula:

$$T_{normative} = \sum_{i=1}^{k} T_b(i)(\widehat{w_i}) \tag{2}$$

where k is the total number of tasks provided to the vehicle b. T_b represents the normalized value of the responses provided by b such that $0 < T_b < 1$. Weights for each task are assigned by the developer depending on the complexity and computation involved in the task. It is to be noted that the value of $T_{normative}$ lies in the range $0 < T_{normative} < 1$.

Once the cognitive and normative components have been computed, the overall transient trust score is given by

$$T_{transient} = T_{cognitive} \circledast T_{normative} \tag{3}$$

VII. Illustrative Examples of the Design

In this section, we will explain the use of specialized NDN names for fulfilling the communication requirements among the entities. In this section, we describe several target vehicular networking applications, network messages, and proposed NDN naming conventions.

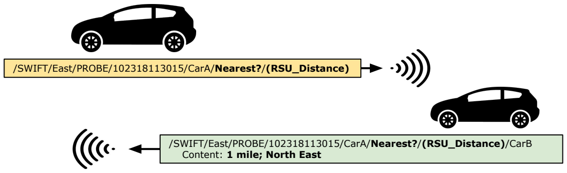
/SWIFT/East/PROBE/102318113015/CarA/**Nearest?/(RSU_Distance)**
/SWIFT/East/PROBE/102318113015/CarA/**Nearest?/(RSU_Distance)**/CarB
Content: **1 mile; North East**

Fig. 4: Spatio-temporal task: Identifying nearest RSU

As an example for a formulated normative task, we consider a spatio-temporal question requesting the distance of the nearest Road-Side Unit (RSU). Figure 4 shows the various exchanges between Car A and Car B. Car A sends out an interest packet with the Probing request asking for the distance of the nearest RSU. The interest packet has various components highlighting the application pertaining to which the message is being transmitted, the direction and the timestamp at which the packet is transmitted and finally the request shown by "`/Nearest?`". Any car that receives this interest packet and is willing to participate can reply with the appropriate content.

Car B, which has received this interest packet, replies with the content that states that the nearest RSU is at a distance of 1 mile in the North Eastern Direction. Based on the guidelines set, Car A computes the value of T_b for Car B.

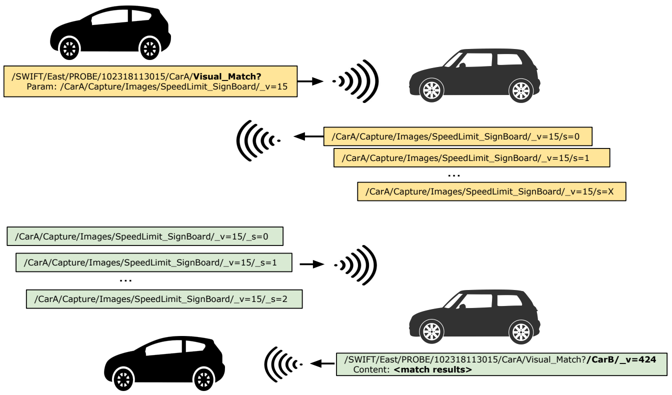
/SWIFT/East/PROBE/102318113015/CarA/Visual_Match?
Param: /CarA/Capture/Images/SpeedLimit_SignBoard/_v=15
/CarA/Capture/Images/SpeedLimit_SignBoard/_v=15/s=0
/CarA/Capture/Images/SpeedLimit_SignBoard/_v=15/s=1
...
/CarA/Capture/Images/SpeedLimit_SignBoard/_v=15/s=X
/CarA/Capture/Images/SpeedLimit_SignBoard/_v=15/_s=0
/CarA/Capture/Images/SpeedLimit_SignBoard/_v=15/_s=1
...
/CarA/Capture/Images/SpeedLimit_SignBoard/_v=15/_s=2
/SWIFT/East/PROBE/102318113015/CarA/Visual_Match?/CarB/_v=424
Content: <match results>

Fig. 5: Visual Matching task

Similarly, Figure 5 depicts another complex task that can be used by the car to compute the normative component of swift trust. Car A in this instance sends out an interest packet requesting the surrounding vehicles to perform a pattern/image match of the specific signboard. On receiving such a request, the interested cars respond with interest packets requesting for the image to be matched. Car A sends out the data packet with the image it wants the surrounding cars to work. Car B, one of the cars interested in performing the computation on receiving the image from Car A queries its internal sensors (like a camera) to capture the particular image in question and thus use it for the matching process. Car B then would perform the matching operation and return the result to Car A as a data packet with the content specifying if it is a match or not. Car A could alter the images being sent and based on its knowledge of if the image/pattern should match, can determine the trustworthiness of the Car that responds.

After all the tasks have been completed, the vehicle computes the trust scores based on the cognitive and normative component values it has aggregated for a particular vehicle. If the trust score thus computed exceeds a set threshold defined by the developer, the car will transmit an interest to collaborate in a lane change. The trust scores thus computed for individual vehicles can be stored in a ledger and compared for reciprocity and thus lead to building long standing reputation values.

VIII. Security and Privacy Threats

In vehicular communication environments, we encounter malicious nodes that intend to attack and bring down the system/network. Deploying an NDN based approach handles some of the attacks. However, the content-centric approach raises the possibilities of encountering newer and more complex attacks/threats. A list of possible threats/attacks with potential counter-measures is provided below.

a) Denial of Service (DoS): Malicious vehicles could send multiple queries to spam the network. This makes the network unavailable for legitimate users requesting data at the same time. The outcome is an increase in lost packets and exchange of NACK packets in the network. NDN solutions to counter the DoS and Distributed Denial of Service (DDoS) attacks as highlighted in [10], [11]. Other solutions include limiting the number of outgoing interests to a threshold above which the vehicle cannot transmit new interests until they existing interests have been satisfied.

b) Replay: As explained earlier, every vehicle can assume multiple roles depending on the scenario. A vehicle can transmit interest packets with the intention to identify trustworthy neighbors and simultaneously be answering the requests of other neighbors. There is thus a possibility where some of the vehicles replay the responses from other vehicles to gain a trustworthy status. Timestamps along with nonce's and other freshness metrics are possible counter-measures.

c) Collusion: Vehicles with malicious intent can operate alone or with the help and support of other surrounding peers to either wage any or multiple of the attacks mentioned above trying to break down the network. A simple example could be in vehicles trying to falsify information and gain access to the network.

d) Fake Data Injection (Cheating with Sensor Information): Attackers try to alter their perceived position, speed, direction, etc. to escape liability, notably in the case of an accident. In the worst case, colluding attackers can clone each other and harness full trust of the target vehicle.

e) ID disclosure: To track the location as in a *Big Brother* like scenario, wherein a global observer constantly monitors trajectory information of targeted vehicles. This data could later be used to profile the user and try to infect the vehicles with malware.

IX. Related Works

Trust bootstrapping as defined earlier is a mechanism of assigning trust rates for new devices and services in a network and thus compute the trustworthiness of the entity. This process is considered a part of the trust-building phase and is performed among entities with little or no prior interactions. Earlier works in this field approached this process by assigning default values which will be altered later to either increase or decrease based on the model and criteria introduced in [12]. Our work, similarly to a small portion of the existing proposals, tries to build a reputation based on the interactions among the entities.

The concept of community based bootstrapping is discussed in [13]. The dependence of the community-based approaches is one of the limitations of this work. A user should be able to trust a service before its invocation without requiring the existence of a community that evaluated the service in the past. We have addressed this issue in this paper. Another community-based approach is seen in [14] where information is aggregated to calculate the probability that the next newcomer will cheat. The main limitation here is the reliance on other entities and their interaction to reflect on a new entity joining the node.

The origin of Trust models can be rooted back to [12]. Works on proactive means of assigning reputation scores to new entities can be seen in [15]. The approach discussed is on the reputation of peers based on pro-active interactions in a collusion based environment.

X. Conclusion

Secure communication among social objects is necessary for accomplishing many task-oriented applications. To make this possible, the social objects need to trust each other at least for short durations during the communication. The proposed design based on Swift trust for vehicular networks should help in accomplishing complex tasks like lane change maneuvers. The hierarchical naming and security advantages provided by NDN makes the proposed design robust. The security and privacy issues specified in the paper offer many open questions to be addressed and is a motivation for our future work.

References

[1] A. Rowstron and G. Pau, "Characteristics of a vehicular network," *University of California Los Angeles, Computer Science Department, Tech. Rep*, pp. 09–0017, 2009.

[2] D. Murthy, A. Rodriguez, and J. Lewis, "Examining the formation of Swift Trust within a scientific global virtual team," in *Proc. of International Conference on System Sciences (HICSS)*, 2013.

[3] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, P. Crowley, C. Papadopoulos, L. Wang, B. Zhang *et al.*, "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[4] G. Grassi, D. Pesavento, L. Wang, G. Pau, R. Vuyyuru, R. Wakikawa, and L. Zhang, "Acm hotmobile 2013 poster: vehicular inter-networking via named data," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 17, no. 3, pp. 23–24, 2013.

[5] B. Parno, J. M. McCune, and A. Perrig, "Bootstrapping trust in commodity computers," in *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 414–429.

[6] S. K. Ramani and S. Iyengar, "Evolution of sensors leading to smart objects and security issues in iot," in *International Symposium on Sensor Networks, Systems and Security*. Springer, 2017, pp. 125–136.

[7] L. P. Robert, A. R. Denis, and Y.-T. C. Hung, "Individual swift trust and knowledge-based trust in face-to-face and virtual team members," *Journal of Management Information Systems*, vol. 26, no. 2, pp. 241–279, 2009.

[8] S. K. Ramani, R. Tourani, G. Torres, S. Misra, and A. Afanasyev, "Ndn-abs: Attribute-based signature scheme for named data networking," in *Proceedings of the 6th ACM Conference on Information-Centric Networking*, 2019, pp. 123–133.

[9] G. Grassi, D. Pesavento, G. Pau, L. Zhang, and S. Fdida, "Navigo: Interest forwarding by geolocations in vehicular named data networking," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a*. IEEE, 2015, pp. 1–10.

[10] A. Compagno, M. Conti, P. Gasti, and G. Tsudik, "Poseidon: Mitigating interest flooding ddos attacks in named data networking," in *Local Computer Networks (LCN), 2013 IEEE 38th Conference on*. IEEE, 2013, pp. 630–638.

[11] P. Gasti, G. Tsudik, E. Uzun, and L. Zhang, "Dos and ddos in named data networking," in *Computer Communications and Networks (ICCCN), 2013 22nd International Conference on*. IEEE, 2013, pp. 1–7.

[12] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on*. IEEE, 1996, pp. 164–173.

[13] Z. Malik and A. Bouguettaya, "Reputation bootstrapping for trust establishment among web services," *IEEE Internet Computing*, no. 1, pp. 40–47, 2009.

[14] M. Feldman and J. Chuang, "The evolution of cooperation under cheap pseudonyms," in *E-Commerce Technology, 2005. CEC 2005. Seventh IEEE International Conference on*. IEEE, 2005, pp. 284–291.

[15] G. Swamynathan, *Towards reliable reputations for distributed applications*. University of California at Santa Barbara, 2008.