UAV-VANET Authentication for Real-Time Highway Surveillance

Otto B. Piramuthu
Computer Science, UIUC
Urbana, Illinois 61801, USA
obp2@illinois.edu

Matthew Caesar
Computer Science, UIUC
Urbana, Illinois 61801, USA
caesar@illinois.edu

Abstract

Unmanned aerial vehicles (UAVs) or drones have the potential to supplant helicopters in real-time highway surveillance applications due to cost, form factor, and other considerations. The wireless medium used for communication has the potential to expose a fleet of drones en route to surveillance to link failures and attacks on passed messages. Given the sparse topology, messages among UAVs, vehicles, and trusted authority could be transmitted through collaboration among UAVs and vehicles. Since vehicles and drones in a highway environment are mobile, related ad hoc network is continuously updated to account for reachability of transmitted signals. It is also necessary to authenticate the drones and vehicles to ensure that the transmitted messages are uncorrupted and trusted. To accommodate processing power and mobility constraints, we develop lightweight authentication protocols that facilitate secure message transfer. We also evaluate the security properties of these protocols.

CCS Concepts

• **Security and privacy** → **Authentication**;

Keywords

VANET, authentication, unmanned aerial vehicle (UAV)

ACM Reference Format:
Otto B. Piramuthu and Matthew Caesar. 2022. UAV-VANET Authentication for Real-Time Highway Surveillance. In *The 37th ACM/SIGAPP Symposium on Applied Computing (SAC '22), April 25–29, 2022, Virtual Event, .* ACM, New York, NY, USA, Article 4, 7 pages. https://doi.org/10.1145/3477314.3507021

1 Introduction

With the increase in popularity of unmanned aerial vehicles (UAVs) in a wide variety of application areas [1][8][14] that include aerial photography, disaster management [9], geographic mapping of inaccessible terrains, package delivery, and search and rescue operations, it is only natural to consider even more possible use for these vehicles. One such application is aerial surveillance of highways [4] to facilitate location, identification, and summon help in accident situations as well as in normal day-to-day highway surveillance operations. UAVs or drones are resource-constrained due to their form factor and weight and are generally light in terms of battery power as well as computational resources that include processing power and long-distance communication capabilities. These constraints necessitate the use of a network of drones in which each drone can communicate (i.e., reachable) at least with one other drone or a base station during most of its operational duration [15][16][19]. The rather sparse and dynamic topology associated with UAVs and their constrained battery power leads to frequent breaks in their links, resulting in related communication challenges. Both single-hop and multi-hop protocols are used, depending on the distance between message source and destination. To help facilitate the deployment of UAVs in highway surveillance scenarios, cooperation with Vehicular Ad hoc Networks (VANETs) is a possible option.

With the cooperation of UAVs and VANETs, the messages that are passed among the different entities (base stations, drones, RSUs, and vehicles) play a significant role in the seamless operation of this combined UAV-VANET system. It is therefore critical to ensure that these messages are trusted and timely. From a trust-based perspective, it is necessary to ensure that the messages are from a trusted (drone, TA, or vehicle) source and that none of these messages are corrupted by an unauthorized party. An important step in this process is the authentication of all communicating entities, while ensuring that none of the messages reveal any critical information to an adversary. These messages are therefore encrypted so that any given message seems random to an eavesdropper. To this end, we develop lightweight [17] authentication protocols that help safely deliver messages between any two entities in the UAV-VANET system. Specifically, the developed protocols ensure secure transmission of a generated message from the message-source entity (e.g., drone or vehicle) to its destination (e.g., base station or RSU) in a multi-hop network by not revealing any sensitive component in the message. The only entities that are privy to the sensitive message content are the source and the intended destination nodes of that message. We also develop an authentication protocol that securely delivers message from an RSU or base-station to vehicles or drones.

We present a review of lightweight VANET protocols in the next section. The proposed protocols are presented in the following section, beginning with the system model, which includes the adversary model, related assumptions, and security properties. This is followed by the developed protocols and discussion on their security properties. We conclude the paper in Section 4.

2 Lightweight VANET Authentication Protocols

The highly mobile nature of vehicles constrains VANET authentication protocols to be computationally lightweight and quick with minimal number of communicated messages. Therefore, a majority of published VANET authentication protocols use symmetric key

SAC '22, April 25–29, 2022, Virtual Event,

ACM ISBN 978-1-4503-8713-2/22/04…$15.00
https://doi.org/10.1145/3477314.3507021

cryptography as the computational complexity of public key cryptography is generally several orders of magnitude higher than that of symmetric key cryptography. Extensive use of hash functions can render even symmetric key cryptography to be computationally complex as hash functions can be highly computationally complex. However, even VANET authentication protocols that specifically claim to be lightweight disregard this aspect and use hash functions [20], elliptic curve cryptography [3], public key cryptography [12], among others.

For example, Al-Shareeda et al. [2] propose a Lightweight Security Without Using Batch Verification Method (LSWBVM) authentication protocol that uses elliptic curve cryptography with hash functions during mutual authentication. To verify a large number of messages in a high traffic density area, they use single instead of batch verification. Li et al. [10] propose a lightweight authentication protocol for VANET in which every message includes at least one hash function component. Mansour et al. [12] propose a lightweight group key management protocol that is based on public key cryptography which decouples initialization from group key computation and performs the operations offline. Public key cryptography is generally not known to be lightweight. Since the proposed protocol does not attempt to alleviate associated computational complexity, the veracity of the lightweight claim is unclear. Nandy et al. [11] purport to develop an enhanced lightweight and secure authentication protocol (ELSAP) for V2V Communication in VANETs. Their protocol performs mutual authentication with the use of hash functions in multiple terms in each passed message. Naresh et al. [13] propose a lightweight framework for authentication in VANETs with the use of elliptic curve cryptography for two-party key agreement and dynamic group key agreement. Every message in their protocol uses multiple hash functions. Sikarwar et al. [18] present a lightweight authentication and batch verification scheme (LABVS) for VANET using a bilinear map and one-way hash function (SHA-1). They observe that one-way hash functions fail to provide sufficient security and therefore resort to the use of bilinear pairing which is relatively more computationally complex. Vasudev et al. [20] propose a lightweight mutual authentication protocol for use in Internet of Vehicles and evaluate their protocol against eleven different attack scenarios. Despite their claims on lightweight as the novelty, every message that is passed in their protocol has at least a one-way hash function component. It is clear that extant VANET authentication protocols are not lightweight, despite associated claims. We address this void and develop lightweight UAV-VANET authentication protocols.

3 The Proposed Protocols

We consider the required characteristics before presenting the authentication protocols. Throughout the paper, the wireless communication channels are assumed insecure.

3.1 System Model

Each of the proposed authentication protocols should possess the following characteristics: (1) it must have a small number of messages, as each message potentially provides additional clue(s) on secret information to an attacker, (2) no identification information should be transmitted in the public, to prevent the possibility of tracking and tracing (3) randomness must be incorporated in each sent message to dissuade replay attacks, (4) nonrepudiation of sent messages and associated content, and (5) resist message forgery to ensure that its source is legitimate and that its payload is unaltered by an unauthorized party. The goals are to ensure correct identification of the vehicle or drone, protect the privacy and security of the vehicle or drone, and ensure that none of the messages are tampered by adversaries.

3.2 Security Goals

We consider the important security requirements in VANETs that include authenticity, availability, confidentiality, and integrity.

Authenticity: This facet ensures that the recipient trusts the identity of the claimed message source and the message source trusts the identity of the intended message destination entity.

Availability: This facet ensures uninterrupted communication access to all entities in range. When such access is not available, the focal entity immediately recognizes that its message was not received by the intended recipient(s) or the recipient's response was blocked.

Confidentiality: This facet of security goal ensures information protection from unauthorized access. A shared secret key is known only to the entities sharing that key and no other entity. Vehicle anonymity is maintained and its actual identity is known only to the trusted authority.

Integrity: This facet ensures that only authorized entities are allowed to modify stored or transmitted data. All received messages are guaranteed to be tamper-free during transit. A related condition is nonrepudiation of sent and received messages and associated content by any VANET entity (vehicle, TA).

3.2.1 Adversary Model

Possible threats in a UAV-VANET environment could primarily come from manipulated messages. Since we use location and time information, manipulation by unauthorized entities is a possibility. Other threats include any attack that results in impersonation of base-station, drone, RSU, or vehicle.

3.2.2 Security Model Assumptions

The adversary is assumed to follow the Dolev-Yao intruder model [6] with the ability to freely block, eavesdrop, inject, and modify messages that are passed between any two UAV-VANET entities. The trusted authority (TA) cannot be compromised and is the only entity that knows the real identity of each entity (vehicle, drone). The TA is the only entity that is authorized to authenticate vehicles and drones. The following security properties are assumed.

- The trusted authority cannot be compromised, whereas the vehicles and drones can be compromised and therefore cannot be trusted.
- Adversaries can monitor, block, eavesdrop, and modify any message(s) passed between vehicles and drones as well as inject new message(s) in the entity-entity (e.g., vehicle-vehicle, drone-drone, vehicle-drone) wireless channel.
- Adversaries cannot retrieve any shared secret (private) keys from transmitted messages. Adversaries also cannot decrypt

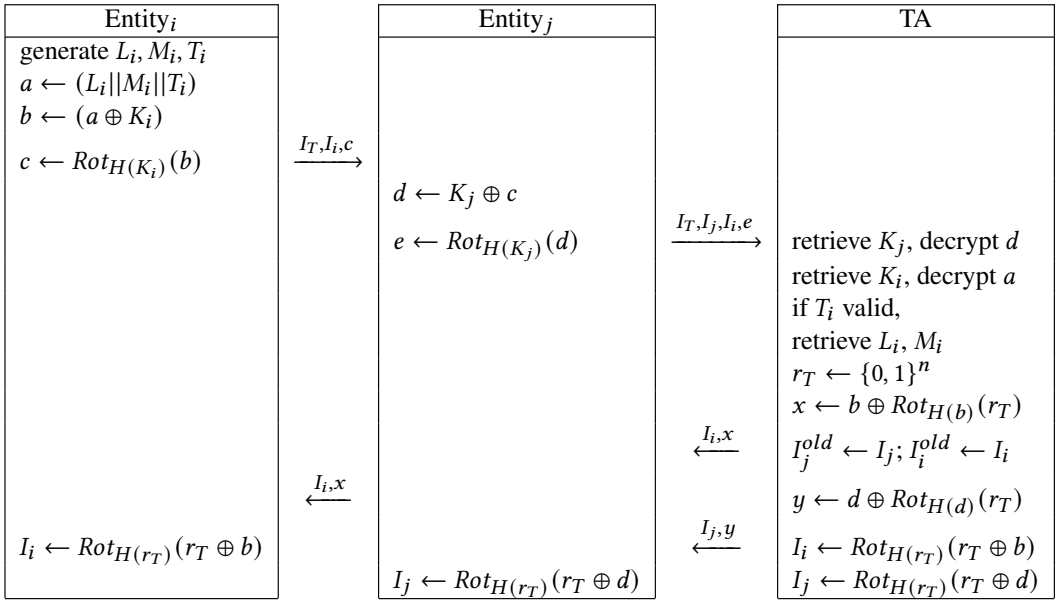

Figure 1: Protocol for message from entity i to TA

any of the message(s) passed in the entity-TA channel and retrieve any of its components

3.2.3 Security Properties

The protocol satisfies the following properties.

Correctness: A drone or vehicle cannot falsely claim to be present at a given location and time.

Drone/Vehicle Anonymity: As drone- or vehicle-generated information may be sensitive, its permanent identification information must not be known to an unauthorized entity.

Untraceability: The messages in the protocol are sufficiently randomized to prevent tracking and tracing of drones or vehicles.

Resistance to Replay Attacks: An attacker cannot compromise the protocol by replaying messages.

Resistance to Impersonation Attacks: The authentication protocol ensures that base-stations, drones, vehicles, and RSUs are not impersonated.

3.3 Authentication Protocols

We develop two authentication protocols for the VANET environment that also includes drones. The first protocol we present is that for securely passing messages from an entity (drone, vehicle) to a trusted authority. The second protocol we present is that for securely passing messages from a trusted authority to an entity (drone, vehicle). We first present the notation we use in the rest of this paper.

Entity	drone or vehicle
TA, I_T	trusted authority and its identity
r_T	TA-generated nonce
I_i, I_j	anonymous identity of entity i,j
L_i, L_j	entity i, j's location coordinates
M_i, M_T	messages from entity i, TA
T_i, T_T	time stamp from entity i, TA
K_i	shared (with TA) key of entity i
$H(a)$	Hamming weight of a
$Rot_{H(a)}(X)$	right-rotate X by $H(a)$
$\|\|$	concatenation operator
$\oplus$	exclusive-OR operator

We first present the developed authentication protocol that helps with secure transmission of a message that is generated by a drone or vehicle. The message generated by a drone could be highway surveillance related and the message that is generated by a vehicle could be related to it joining the zone covered by an RSU or something related to traffic conditions such as an accident or road-blockage.

Figure 1 provides a sketch of this protocol for message (M_i) that is generated by source Entity$_i$, which could be a drone or a vehicle, with the trusted authority (TA) as the intended recipient. Note that the trusted authority includes and represents the base-stations and RSUs, and the keys of the mobile units (UAVs, vehicles) are shared with the trusted authorities. Since the intended message destination (e.g., TA) could be multiple hops away from the source entity, we illustrate a scenario where the message passes through an intermediate entity (here, Entity$_j$) before reaching the TA. When there are several intermediate entities, the message from each entity follows a similar pattern as the ones from Entity$_j$ to the TA.

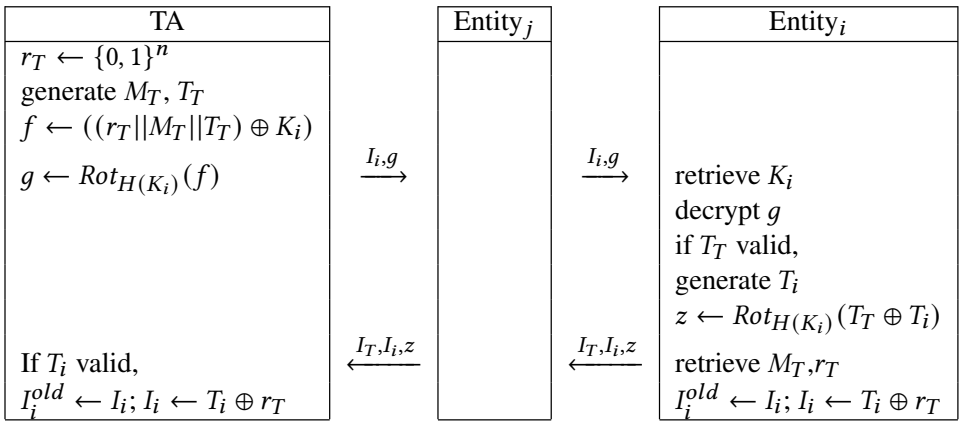

Figure 2: Protocol for message from TA to entity i

The protocol proceeds as follows. The source entity (Entity$_i$) generates message M_i. To ensure that its current location and current time are recorded to prevent attacks from adversaries, it generates/records L_i (its current location) and current time stamp (T_i). Entity$_i$ concatenates L_i, M_i, and T_i as $a \leftarrow (L_i||M_i||T_i)$. It then takes the exclusive-OR of a and its shared key (i.e., K_i) with the trusted authority to generate $b \leftarrow (a \oplus K_i)$. Next, it determines the Hamming weight of its shared key (i.e., $H(K_j)$), which it then uses to right-rotate b to form c (i.e., $c \leftarrow Rot_{H(K_i)}(b)$). It then sends c and anonymous identities (I_T, I_i) to the next entity (here, Entity$_j$). The last entity to forward the message to the trusted authority includes the anonymous identity of all entities that took part in the chain to transmit the message from the origin entity to the TA, which uses this information to decrypt all previous messages in the chain.

As the shared key values are secret and are known only to the entity to which the shared key belongs and TA, inclusion of these keys in the messages ensures that no entity can impersonate another entity. The TA aborts the protocol when it is unable to decrypt (corrupt) messages as this signifies that an adversary had meddled with an intermediate message. Moreover, an adversary cannot originate a message since the protocol requires the adversary's shared secret key and anonymous identity that the adversary does not possess. However, a rogue entity has both an anonymous identity and a shared secret key and can therefore attempt to send an incorrect message. The TA double-checks the veracity of each message through other channels such as through messages or status updates from other nearby entities. The anonymous identities of entities that take part in message transmission are updated after each successful authentication round. Therefore these identities do not reveal any unique information about the entity (drone, vehicle) that an adversary could use to track or trace entities. The TA keeps the previous anonymous identities (here, I_i^{old}, I_j^{old}) to prevent desynchronization attacks.

The protocol in Figure 2 can be used to transmit a message from a trusted authority to a specific entity i, which could be a drone or a vehicle. The protocol begins with the TA generating a nonce (r_T), the message (M_T) it intends to share with entity i, and the time stamp (T_T). The TA concatenates these and takes exclusive-OR with i's shared key (K_i) to form $f \leftarrow ((r_T||M_T||T_T) \oplus K_i)$. This is now right-rotated with the Hamming weight of the shared key (i.e., $H(K_i)$) to generate $g \leftarrow Rot_{H(K_i)}(f)$.

The TA then begins the process of transmitting the encrypted message to its intended destination (i.e., entity i). To this regard, the TA sends g along with the anonymous identity of the recipient (i.e., I_i). Unlike the protocol in Figure 1 which was used to send a message from an entity to a trusted authority, the entities involved in intermediate hops do not modify or update the message received. The intermediate entities just relay the message received to the next entity in the chain to reach the message destination entity i. When the destination entity receives I_i, g, it decrypts g with the use of its shared secret key (K_i) to retrieve f. From f, entity i can readily retrieve M_T and T_T with the help of K_i (i.e., $f \oplus K_i = r_T||M_T||T_T$). It disregards the message if T_T is invalid (i.e., either T_T is sometime in the future or it is more than the expected transmission time from TA, suggesting possible replay attack).

To acknowledge receipt of message M_T, i sends (I_T, I_i, z) to the TA, where I_T in the beginning of the message signifies that the message is meant for the TA. This is similar to Figure 1 where I_T, I_j, I_i signifies that the messages in this chain began with entity i as the source, followed by j, which is followed by TA as the destination. The TA stores the previous anonymous ID value as security against synchronization attacks. As in the protocol in Figure 1, the conversation initiator (here, TA) resends the (r_T, T_T)-updated message if response is not received within a pre-specified amount of time.

3.4 Security Properties

We first discuss the security properties of the protocol in Figure 1 based on the requirements as listed in Section 3.2.3. This protocol follows the *correctness* requirement since the location of the nearby entities (base-stations, drones, RSUs, and vehicles) can be determined by the trusted authority based on previous communication. The message origin entity includes its location and current time stamp along with the message to ensure *correctness*. The *anonymity* of the drones and vehicles that take part in message transfer chains is maintained thanks to the use of ephemeral anonymous identity that is updated after each authentication protocol round. The messages are encrypted with lightweight operators that include concatenation, exclusive-OR, and rotation to generate randomness to prevent

tracking or tracing (i.e., *untraceability*) of the drones and vehicles. The protocol is *resistant to replay attacks* with the inclusion of the time stamp component in the messages. Since time stamp is encrypted, an adversary cannot easily modify this value to that of a later point in time to mount replay attacks. The use of shared keys in the encrypted messages ensures that the entities are *resistant to impersonation attacks* as these keys are not known to adversaries.

We now discuss the security properties of the protocol in Figure 2 based on the requirements as listed in Section 3.2.3. The protocol follows the *correctness* claim since the vehicle does not claim to be at any given position at a given time as the TA is the source of the message and a stationary TA does not have to prove its location. However, a replay attack can result in an incorrect time stamp, which is checked by the destination entity for correctness. As in Figure 1, the permanent identification information is not used in this protocol. We use the anonymous identity which is updated after every successful authentication round. Therefore, *drone/vehicle anonymity* is maintained in this protocol. The messages in the protocol are randomized through encryption to prevent tracking and tracing (i.e., *untraceability*) of the entity by an adversary. The use of time stamp (i.e., T_T) at the origin ensures that the protocol is *resistant to replay attacks*. The use of shared key (K_i), which is known only to the intended destination entity and the trusted authorities, ensures *resistance to impersonation attacks*.

We show the correctness of the proposed protocol when the protocol is in fact correct assuming ideal cryptography through *strand space* [21] following the logic presented in Fábrega et al. [7]. We operationalize this by showing that no entity (e.g., adversary) learns its forbidden facts. To this end, the limitations of the entities are modeled, and these limitations effectively obstruct these entities from inferring the forbidden facts. Since the two proposed protocols are similar in structure, we show the correctness of the protocol to securely pass messages from source i to the trusted authority (Figure 1). The proof for the correctness of the protocol for messages from trusted authority to entity i (Figure 2) is similar in structure and is therefore omitted.

Strand space emphasizes causal interactions among cryptographic protocol participants for state-based analysis of completed protocol runs. A strand space Σ is a set of strands and contains all legitimate executions during the useful lifetime of the protocol of interest and all associated actions of an adversary. A strand is a sequence of message transmission and reception events associated with a legitimate party (principal) which participates in successful completion of the protocol. Each event in a strand is an action of a principal and has associated values (e.g., nonce). For an adversary, a strand includes messages that model associated capabilities. The strand space approach provides clear semantics on the freshness of data items such as nonce which is significant to avoid attacks (e.g., replay attack). The explicit model of adversarial behavior allows for general bounds on abilities of adversaries and detailed insight on the correctness of a protocol and associated assumptions.

A principal can send or receive terms, respectively represented by a positive or a negative sign. The trace of a strand is the sequence of its signed terms. We use P_V to represent the proposed protocol and use guarantees from the responder's and initiator's side through propositions to develop the proof.
We use the following notation.

- $\mathcal{P}, \Sigma$: penetration (i.e., adversarial) strand space, strand space
- T, T_{name}: set of text representing atomic messages
- C: bundle
- t_i^{-1}: inverse (key)
- K_P: keys known to the penetrator (i.e., adversary)
- $\prec$: precedence relationship
- $\sqsubset$: subterm (e.g., $t_0 \sqsubset t_1$)

Definition 1 $(\Sigma, \mathcal{P})$ is an infiltrated strand space if Σ is a strand space and $P \subset \Sigma$ is such that the trace of p is a penetrator trace for all $p \in \mathcal{P}$.

Definition 2 An infiltrated strand space $\mathcal{P}, \Sigma$ is a P_V space if Σ is the union of three kinds of strands. Here, we consider messages between Entity_i and Entity_j as an example with L_i, M_i, and T_i embedded in c as freshly generated items from Entity_i, and r_T embedded in x from TA via Entity_j.

(1) Penetrator strands $s \in \mathcal{P}$
(2) Initiator strands with trace Init[Entity_i, Entity_j, I_T, I_i, c], defined to be $\langle +(I_T, I_i, c), -(I_i, x) \rangle$, where Entity_i, $\text{Entity}_j \in \text{T}_{name}$ but $I_T, I_i, c \notin \text{T}_{name}$
(3) Its complement, the responder strands with trace Resp[Entity_i, Entity_j, I_i, x], defined to be $\langle -(I_T, I_i, c), +(I_i, x) \rangle$, where Entity_i, $\text{Entity}_j \in \text{T}_{name}$ but $I_i, x \notin \text{T}_{name}$

3.4.1 The Responder's Guarantee: Agreement

Proposition 1 Suppose:

(1) Σ is a P_V space and C is a bundle containing a responder's strand s with trace Resp[Entity_i, Entity_j, I_i, x];
(2) $t_i^{-1} \notin K_P$; and
(3) $c \neq x$ and x is uniquely originating in Σ then C contains an initiator's strand t with trace Init[Entity_i, Entity_j, I_T, I_i, c].

We prove this proposition using the following lemmas.

Lemma 1 x, and therefore r_T, originates at the second message (the one from Entity_j).

We know $x \sqsubset \text{Entity}_j$ (node n_o) and the sign for the second message (say, v_o) is positive since it originates from Entity_j. We, therefore, need to verify that x, and therefore r_T, is not in the preceding node (here, Entity_i) in the strand, which is the preceding node on this strand. I.e., $c \neq x$, $x \neq L_i$, $x \neq M_i$, $x \neq T_1$, and $x \neq r_T$. These are all true by definition.

Lemma 2 The set $S = \{\text{n} \in C : x \sqsubset term(n) \wedge v_o \not\sqsubset term(n)\ \}$ has a $\preceq$-minimal node n_2. The node n_2 is regular with a positive sign.

We need to check if n_2 lies on a penetrator strand p.
S. If g h $\sqsubset$ term(m), where m is a positive node on a strand p' of kind S, then g h $\sqsubset$ term($\langle p', 1 \rangle$). Minimality of m in T is contradicted by $\langle p', 1 \rangle \prec$ m.

E.(D.) If g h ⊏ term(m), where m is a positive node on a strand p' of kind E (D, respectively), then g h ⊏ term($\langle p', 2\rangle$). Minimality of m in T is contradicted by $\langle p', 2\rangle \prec$ m.
C. If g h ⊏ term(m), where m is a positive node on a strand p' of kind C and m is minimal in T, then g h = term(m) and p' has trace $\langle -g, -h, +gh\rangle$. This contradicts the minimality of n_2 in S since term($\langle p', 1\rangle$) = term(n_2) and $\langle p', 1\rangle \prec n_2$.

Lemma 3 Node n_2 follows n_1 on the same regular strand t, and term(n_1) = $\{I_i, x\}$

From Lemma 1 and by definition, we know that x, and therefore r_T originates at n_o and its uniqueness in Σ. We also know that $n_2 \neq n_o$ since $v_o \sqsubset term(n_o)$ and $v_o \not\sqsubset term(n_2)$. Therefore, x (or r_T) does not originate at n_2 and there is a node n_1 preceding n_2 on the same strand such that $x \sqsubset term(n_1)$. By the minimality property of n_2, $I_i, x \sqsubset term(n_1)$. Here, I_i, x = term(n_1) since no regular node contains an encrypted term as a proper sub-term.

Lemma 4 The regular strand t containing n_1 and n_2 is contained in C and is an initiator strand.

If t were a responder strand, it would contain only a subsequent negative node. Here, n_2 is a positive node. The last node of t (i.e., n_2, which follows n_1) as well as the previous nodes are contained in C.

Lemmas 3 and 4 prove Proposition 1.

3.4.2 *The Initiator's Guarantee: Secrecy and Agreement*

Proposition 2 Suppose:

(1) Σ is a P_V space and C is a bundle containing an initiator's strand s with trace Init[Entity$_i$, Entity$_j$, I_T, I_i, c];
(2) $t_i^{-1} \notin K_P$; and
(3) L_i, M_i, T_i uniquely originates in Σ then for all nodes $m \in C$ such that $T_i \sqsubset term(m)$ either $(I_T, I_i, c) \sqsubset term(m)$ or $(I_i, x) \sqsubset term(m)$

Proposition 3 Suppose:

(1) Σ is a P_V space and C is a bundle containing an initiator's strand s with trace Init[Entity$_i$, Entity$_j$, I_T, I_i, c];
(2) $t_i^{-1} \notin K_P$; and
(3) L_i, M_i, T_i uniquely originates in Σ then C contains the first two nodes of a responder's strand t with trace Resp[Entity$_i$, Entity$_j$, I_i, x].

The set {m ∈ C : $I_i, x \sqsubset term(m)$ } is non-empty since it contains $\langle s, 2\rangle$. I.e., it contains a minimal member (m_o). Now, the regular strand t can be shown to have trace Resp[Entity$_i$, Entity$_j$, I_i, x] if m_o lies on t. The regular strand t can also be shown to have at least two nodes in C. However, if m_o lies on a penetrator strand t, then t can be shown to be an **E**-strand with trace $\langle -L_i, -M_i, -T_i, +I_i, +x\rangle$. However, this contradicts Proposition 2, which implies that x (or r_T) does not appear in the form shown in node $\langle t, 2\rangle$. A similar reasoning proof can be readily seen for the messages between trusted authority and Entity$_i$ since the messages passed between these two entities (i.e., TA and Entity$_i$) are similar in structure.

4 Discussion and Conclusion

Vehicles that are part of a VANET depend on communication with other entities such as other vehicles, road-side units, and trusted authority to send and receive relevant information. While not all such communication might necessarily precipitate in security or privacy issues, the nature of VANET and associated communication renders these messages to be sensitive toward exposure to unintended parties. Such communication instances therefore need to be secured to prevent their leakage. One of the means to achieve this is through authentication of communicating parties to ensure that source and destination of each message are as intended. Cryptography is commonly used for this purpose.

Despite diligent care taken to encrypt passed messages among VANET entities, the possibility of attacks that reveal sensitive information remains. To inspire confidence in the security and privacy aspects of VANET authentication protocols, it is necessary for such protocols to be resistant against various types of attacks that could possibly be mounted in such systems. We attempt to bridge this void in VANET authentication literature through the proposal of lightweight protocols that consider several types of attacks.

Since vehicles are in motion in VANETs, it is better for authentication protocols to be lightweight and short with minimal number of messages between the authenticating parties. Our review of published VANET authentication protocols revealed that while there are indeed some VANET authentication protocols that claim to be lightweight, they all use expensive operations and/or have several message exchanges between the authenticating parties for successful protocol completion. To this end, our goal is to develop lightweight VANET authentication protocols with minimal number of required messages.

We considered the integration of VANET and UAVs for seamless communication among drones and vehicles to facilitate real-time highway surveillance. Specifically, we developed authentication protocols that securely transfer messages from drones and vehicles to trusted authority (base-stations, RSUs) and vice versa. Security of these messages and associated entities is critical to ensure a trustworthy system. Since drones are resource-constrained, the developed protocols are lightweight and compact and can be operationalized quickly with minimal computational burden on the participating entities. We considered the security properties of the proposed protocols through informal walk-through as well as formal strand space analysis.

References

[1] G. Ahmed, T.R. Sheltami, A.S. Mahmoud, M. Imran, M. Shoaib (2021) A Novel Collaborative IoD-Assisted VANET Approach for Coverage Area Maximization. *IEEE Access*, 9, 61211-61223
[2] M.A. Al-Shareeda, M. Anbar, M.A. Alazzawi, S. Manickam, A.S. Al-Hiti (2020) "LSWBVM: A Lightweight Security Without Using Batch Verification Method Scheme for a Vehicle Ad Hoc Network." *IEEE Access*, 8, 170507-170518.
[3] T. Alladi, S. Chakravarty, V. Chamola, M. Guizani (2020) "A lightweight authentication and attestation scheme for in-transit vehicles in IoV scenario." *IEEE Transactions on Vehicular Technology*. 69(12), 14188-14197.
[4] N. Bashir, S. Boudjit (2020) An Energy-Efficient Collaborative Scheme for UAVs and VANETs for Dissemination of Real-Time Surveillance Data on Highways. *IEEE 17th Annual Consumer Communications & Networking Conference*

(CCNC)

[5] T. Beth, Y. Desmedt (1990) Identification Tokens - or: Solving the Chess Grandmaster Problem. *Advances in Cryptology-CRYPTO'90*, Springer LNCS 537, 169-176.

[6] D. Dolev, A.C. Yao (1983) On the Security of Public Key Protocols. *IEEE Transactions on Information Theory*, 29(2), 198-207.

[7] F.J.T. Fábrega, J.C. Herzog, J.D. Guttman (1999) Strand spaces: Proving security protocol correct. *Journal of Computer Security*, 7, 191-230.

[8] F. Guerriero, R. Surace, V.Loscrí, E.Natalizio (2014) A multi-objective approach for unmanned aerial vehicle routing problem with soft time windows constraints. *Applied Mathematical Modelling*, 38(3), 839-852.

[9] K. Hazra, V.K. Shah, M. Bilal, S. Silvestri, S.K. Das, S. Nandi, S. Saha (2020) Designing Efficient Communication Infrastructure in Post-disaster Situations with Limited Availability of Network Resources. *Computer Communications*, 164(1), 54-68.

[10] X. Li, T. Liu, M.S. Obaidat, F. Wu, P. Vijayakumar, N. Kumar (2020) "A Lightweight Privacy-Preserving Authentication Protocol for VANETs." *IEEE Systems Journal*, 14(3), 3547-3557.

[11] T. Nandy, M.Y.I.B. Idris, R.M. Noor, A.K. Das, X. Li, N.A. Ghani, S. Bhattacharyya (2021) "An enhanced lightweight and secured authentication protocol for vehicular ad-hoc network." *Computer Communications*, doi: https://doi.org/10.1016/j.comcom.2021.06.013.

[12] A. Mansour, K.M. Malik, A. Alkaff, H. Kanaan (2021) "ALMS: Asymmetric Lightweight Centralized Group Key Management Protocol for VANETs." *IEEE Transactions on Intelligent Transportation Systems*, 22(3), 1663-1678.

[13] V.S. Naresh, S. Reddi, V.D. Allavarpu (2021) "Provable secure dynamic lightweight group communication in VANETs." *Transactions on Emerging Telecommunications Technologies*, e4273. https://doi.org/10.1002/ett.4273

[14] E. Natalizio, V. Loscri, E. Viterbo (2008) Optimal placement of wireless nodes for maximizing path lifetime. *IEEE Communications Letters*, 12(5), 362-364.

[15] R.A. Nazib, S. Moh (2020) Routing Protocols for Unmanned Aerial Vehicle-Aided Vehicular Ad Hoc Networks: A Survey. *IEEE Access*

[16] O.S. Oubbati, A. Lakas, F. Zhou, M. Gunes, N. Lagraa, M.B. Yagoubi (2017) Intelligent UAV-Assisted Routing Protocol for Urban VANETs. *Computer Comms*.

[17] H. Sedjelmaci, M.A. Messous, S.M. Senouci, I.H. Brahmi (2019) Toward a lightweight and efficient UAV-aided VANET. *Transactions on Emerging Telecommunications Technologies*, 30(8).

[18] H. Sikarwar, A. Nahar, D. Das (2020) "LABVS: Lightweight Authentication and Batch Verification Scheme for Universal Internet of Vehicles (UIoV)." *IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, 1-6, doi: 10.1109/VTC2020-Spring48590.2020.9129180.

[19] F.B. Sorbelli, S.K. Das, C M. Pinotti, S. Silvestri(2018) Range based Algorithms for Precise Localization of Terrestrial Objects using a Drone. *Pervasive and Mobile Computing*, 48, 20-42.

[20] H. Vasudev, V. Deshpande, D. Das, S.K. Das (2020) "A Lightweight Mutual Authentication Protocol for V2V Communication in Internet of Vehicles." *IEEE Transactions on Vehicular Technology*, 69(6), 6709-6717.

[21] F. Yang, S. Escobar, C. Meadows, J. Meseguer, S. Santiago (2016) Strand Spaces with Choice via a Process Algebra Semantics. *Proceedings of the 18th ACM International Symposium on Principles and Practice of Declarative Programming (PPDP)*, 76-89.