Secure and Efficient Context-Aware Localization of Drones in Urban Scenarios

Vishal Sharma, Dushantha Nalin K. Jayakody, Ilsun You, Ravinder Kumar, and Jun Li

The authors present a novel solution that is capable of securing the context information for sharing 3D waypoints between UAVs. The proposed approach achieves optimal localization through hierarchical context-aware aspect-oriented Petri nets while being powered by a novel drone context-exchange protocol for security validations.

Abstract

Drone swarming involves multiple unmanned aerial vehicles (UAVs), which are able to manoeuver autonomously, providing a vast range of surveillance applications such as traffic evaluations, driver monitoring, disaster management, temporary network support, and pedestrian tracking. All these applications are an integral part of urban surveillance. In other words, cooperation between multiple drones can facilitate urban surveillance while being able to provide high-quality 3D visualization of the surroundings. This 3D representation is driven by the initiation of accurate and non-overlapping waypoints. Such efficient localization depends on the type of context and its security validation by the receiving entities. For example, a highly burdened context with negligible security is of limited use. This article presents a novel solution that is capable of securing the context information for sharing 3D waypoints between UAVs. The proposed approach achieves optimal localization through hierarchical context-aware aspect-oriented Petri nets while being powered by a novel drone context-exchange protocol for security validations.

Drones and Urban Surveillance

Unmanned aerial vehicles (UAVs) or drones are one of the most versatile units for urban surveillance.[1] Urban scenarios involve complex geographical terrains with a large number of buildings, which makes it difficult for UAVs to manoeuvre in a swarm. Multiple UAVs in cooperative formation can cover a vast urban area without any collisions as well as search overhead. Cooperative formation involves mutual assistance between the UAVs and the underlying infrastructure for resolving a particular task [1].

Autonomous operations over UAVs make it possible to provide an immense range of applications including traffic evaluations, driver monitoring, disaster management, temporary network support, pedestrian tracking, and so on [2]. All of these are subject to scalability and depend on the reachability of UAVs. Cooperative swarming can provide better support compared to a single UAV system, whereas it faces several computational, operational, and management issues demanding real-time solutions [3, 4].

Another aspect of drone swarming involves support for the underlying communication network along with search, tracking, and data acquisition, as shown in Fig. 1. Cooperative drones are one of the key entities in the upcoming 5G era [1]. UAVs own a special ability to handle many tasks, whose operation and success depend on the payload capacity and configuration of these vehicles.

With a growing market, UAVs present a potential business opportunity for industries and many startups. Various multi-nationals such as Google, Facebook, Amazon, and Boeing have started focusing on developing their own fleets of aerial vehicles for specialized missions involving civilian as well as military activities. The perception of drones as predators has overshadowed their other capabilities, including UAV-to-UAV (U2U) support for cellular networking, device-to-device communications, urban computing, and so on [5]. In the context of urban scenarios, drones are seen as "eyes in the sky," especially targeting near-site evaluations.

The flying range of UAVs varies for each country and depends on the respective countries' aviation guidelines. For example, the United States and European Union have already started planning on the permissible altitude of UAVs. Soon, UAVs will be a common object in the sky supporting our daily activities. Focusing on UAV swarming in urban scenarios, it is mandatory to devise cooperative algorithms for collision avoidance. Swarming activities like trajectory planning [6] and location selection [7] depend on the non-overlapping waypoints of each UAV as well as the geographical terrain. Accordingly, both the localization and the security of waypoints for each UAV are of extreme importance to form a cooperative UAV swarm in urban scenarios [8].

Limitations of Drones in Urban Scenarios

The concept of drone networks has evolved over the years. However, there are certain limitations associated with them. They are as follows.

Lifetime: Proper energy harvesting or power-efficient green approaches can help address issues related to battery losses and frequent replacements of batteries for UAVs.

Security: There are several security issues related to UAV-assisted urban surveillance, including potential attacks such as UAV hijacking, signal jamming, and waypoint alterations.

Topology: Since a large number of aerial nodes will serve an area, a decision on the formation of topology is a crucial task.

[1] Drones and UAVs are used interchangeably in this article.

Digital Object Identifier: 10.1109/MCOM.2018.1700434

Vishal Sharma and Ilsun You are with Soonchunhyang University; Dushantha Nalin K. Jayakody is with the National Research Tomsk Polytechnic University; Ravinder Kumar is with Thapar University; Jun Li is with Nanjing University of Science and Technology.

0163-6804/18/$25.00 © 2018 IEEE

Network Management: UAVs are capable of flying autonomously, but they need a centralized body, control station, or network node for operations in an urban environment. Thus, management involving command and control over the aerial nodes is a huge challenge for companies looking at their use in future networks.

Line of Sight: To communicate, each UAV should maintain a line of sight (LoS). Thus, non-availability of LoS can cause undesirable interruptions in the operations. LoS plays a vital role in scenarios involving UAVs as direct facilitation of links between the surveillance receiver and transmitter. Large-scale buildings and objects can affect the availability of LoS; thus, the control algorithms should be efficient enough to maintain the operation of UAVs even in the absence of appropriate LoS.

Regulatory Concerns: As each country is governed by their own specific set of laws, the operation of UAVs needs to be formulated for country-specific national legislation systems. National security, military concerns, and social impact should be addressed.

Requirements for Drone Localization in Urban Scenarios

Drones are one important entity for reconnaissance in urban scenarios. Despite the advantages and applications of UAVs, there are certain requirements associated with their error-free operation and deployment, which include:

- Formation of a common frame of reference for providing accurate location coordinates
- Efficient solutions for UAVs to infrastructure and U2U collision avoidance
- Handling signal interference with the underlying communication networks
- 3D imaging in developed cities
- Control of individual vehicles and prevention of hijacking
- Observing the aviation standards for a particular geographical location
- Efficient and accurate algorithms for generating waypoints for autonomous movement
- Local landing sites in the case of unfavorable flying conditions

Problem Statement and Our Contribution

There are many approaches that emphasize the 3D localization of drones in indoor as well as outdoor scenarios, such as spatially secure communication [9], PCA-based localization [10], cooperative UAVs [11], and WiFi-assisted localization [12]. These approaches are effective in supporting 3D manoeuverability of UAVs. But they are unable to support dynamic security on the basis of context between multiple UAVs intended for the same tasks, especially in urban scenarios. Here, context refers to the information and properties of UAVs and network entities required for each other's identification. Dynamic security refers to the validations of localization points, which keep on changing with the manoeuvers of drones. The threat implications of dynamic security on the basis of context include capturing of UAVs or contextual information, alteration of waypoints, unauthorized access to drone messaging network, signal jamming, and initiation of other known cyber attacks. These threats can be addressed by validating the context as well as U2U communication even in the attacker environment. Such an approach is necessary to be scalable in terms of UAVs as well as context while not causing excessive overheads during the flight. To the best of the authors' knowledge, none of the existing solutions focuses on securing context-aware localization of drones in the urban scenarios.

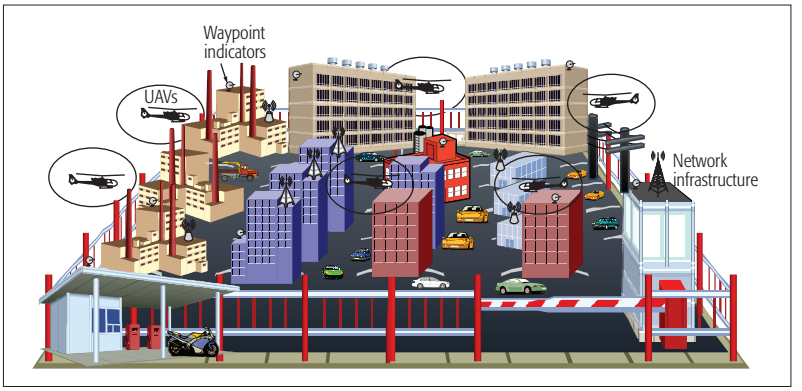


Figure 1. An illustration of cooperative drones in an urban scenario.

In order to timely handle the aforementioned issues, this article aims at designing an efficient and secure solution by resorting to 3D context-aware localization of multiple aerial vehicles in urban environments. The proposed approach utilizes hierarchical context-aware aspect-oriented Petri Nets for context sharing and state identification of each UAV in the urban swarm. Moreover, it is powered by a novel protocol, which provides security of context as well as the location of each UAV in an attacker environment.

Hierarchical Aspect-Oriented Petri Nets

Petri nets are the combination of places, transitions, and arcs, often defined as a triple, (P, T, R), where P denotes places, T denotes transitions, R denotes the arcs between the places and transitions. Circles represent the places, solid bars represent the transitions, and directional arrows represent the arcs. Note that sets containing P and T are disjoint and do not overlap. Each arc governs the tokens, and a transition enables or disables itself according to the system model. The places can define input or output according to the direction of arcs and a transition can fire only if there are enough tokens in the input place to match the need of the output place. Places are only connected to transitions and vice versa [13].

In aspect-oriented Petri nets [14], the arcs serve as the aspects denoted by context C. The transition will fire only if the context expected on the arc between the transition and output place is available from the contexts available on the input arcs between the transition and input places. In aspect-oriented Petri nets, a transition can serve many places, and vice versa, at the same instance.

In hierarchical aspect-oriented Petri nets, which is a novel variant of aspect-oriented Petri nets, another triple, $(\mathcal{P}_A, \mathcal{V}, \mathcal{D})$, connects two or more aspect-oriented Petri nets. Here, $\mathcal{P}_A$ is the number of passes between two or more Petri nets, and for any two Petri nets, $\mathcal{P}_A = \sum P + \sum P'$, where P and P' are the places for the two Petri Nets. $\mathcal{V}$ is the number of validation points, which

The proposed approach does not fall into complex mapping for generating non-overlapping coordinates; rather the proposed approach takes into account the coordinates along with the height and area to generate a 3D cylinder which encircles the entire building.

is half the number of total passes. $\mathcal{D}$ is the decision point, whose value is equal to 1, and increases if there are many exit points in the Petri nets. Note that the passes follow the actual principle of connecting places to transitions only, which is never violated. The passes connect places with an odd degree of connections to the transitions with the required context outputs.

Environment Setup

The proposed approach uses an urban scenario comprising high and densely situated buildings. This approach also relies on the underlying communication network architecture for localization. Each building provides a local frame of reference (LFR) via sensors, which transmit beacons and have all-the-time availability. These beacons support the drones for location awareness by providing the details of area and height of the buildings. In the proposed approach, all the UAVs agree on a centralized coordinating point among LFRs referred to as the point of reference (PoR). The LFRs and PoR help determine the accurate waypoints (safe coordinates) for maneuvering.

Context-Aware Localization for Drones Using Hierarchical Aspect-Oriented Petri Nets

The proposed approach aims at the formation of a secure context-aware solution for localization of drones in the urban scenario by using hierarchical aspect-oriented Petri nets inspired by Xu and Nygard [14]. After selecting a PoR, each UAV starts building its Petri nets model and shares its coordinates with fellow vehicles. The context for drones includes UAV id (U_{id}), LFR id (L_{id}), AP id (A_{id}), coordinates for UAVs (x, y, z), overlap Boolean (O_b), UAVs heading (θ), UAVs speed (S), the adjacency (α) for UAVs and PoR, area (A) and height (H) of buildings, number of UAVs (m), and timestamp (τ). O_b ensures the safety of coordinates for drones to prevent any collision during manoeuvering, where $O_b = 0$ refers to no overlap and $O_b = 1$ refers to an overlap. θ tracks the direction of drones and α provides the information of adjacent UAVs during validation. *P<index>* denotes the places or states, *T<index>* denotes the transitions, and *C<index>* denotes the context. Figure 2 illustrates the Petri nets by using the context from UAVs and the underlying infrastructure. The model functionality of each Petri net includes the following.

Petri Nets for UAVs: Figure 2a presents the aspect-oriented Petri nets for U2U manoeuvers and map construction. The places (*P0–P11*) represent the milestones for drones, transitions (*T0–T8*) represent conditions leading to a particular place by using the drone context (*C1–C28*). Each transition fires once it receives the context from the concerned entity. The concept of transition firing is like the one explained in the introduction to hierarchical aspect-oriented Petri nets. The corresponding tables show the label values of places, transitions, and context. The context values are fixed on the basis of the requirement of a particular transition to fire for reaching the connected place. The Petri nets involve mission inputs that refer to the geographical terrain. The beacon messages harmonize information with all the aerial vehicles. The primary task of this Petri net is to support UAVs with coordinates of other flying vehicles in the context of PoR and then build a map which will help in the generation of the non-overlapping coordinates in an urban scenario.

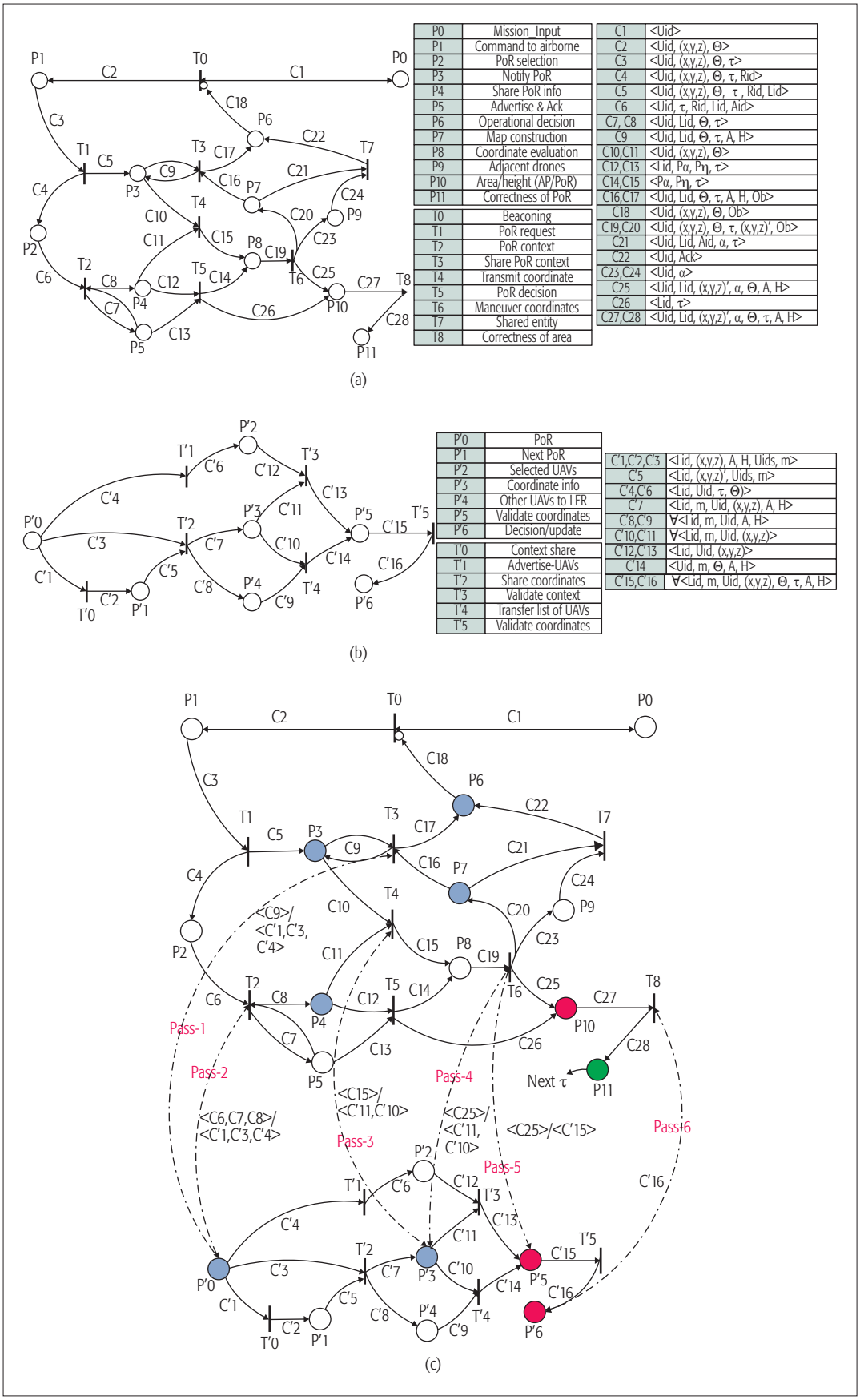
Petri Nets for LFR and APs: Figure 2b presents the self-information sharing between the LFRs and the PoR as fixed in the urban scenario. The places (*P′*0–*P′*6) represent the milestones for infrastructure, transitions (*T′*0–*T′*5) represent conditions leading to a particular place by using the LFR-AP context (*C′*1–*C′*16). These Petri nets emphasize the importance of the information obtained from LFRs and PoR. The model operates cooperatively and supports the sharing of coordinates with UAVs as well as available LFRs. This model provides validation support once included in the previous Petri nets.

Petri nets for the entire urban scenario: Figure 2c presents the hierarchical and dynamic context-aware aspect-oriented Petri nets for infrastructure-assisted localization of drones in the urban scenario. The isolated operation of all the UAVs and LFRs is vulnerable to threats; thus, the hierarchical approach combines the Petri nets from UAVs and LFRs. The hierarchical parts use passes, which are equal to $\sum P - \sum P' + 1$, that is, 6 (12 – 7 + 1). The blue color shows the reference points where both the Petri nets are attached via a transition-place rule like that of simple Petri nets. Red indicates the key validation places in the entire model with green referring to the decision in context. Usually, the hierarchical approach has one decision point, and the number of validation points is equal to half the number of passes.

Appropriate selection of PoR allows securing the UAV system from intruders as the malicious node is always unaware of the actual location of the drones, which is set using the dynamic decision for every PoR. These PoRs update after a certain timestamp or identification of a possible threat. There might be a scenario that has a compromised PoR; such a scenario is hazardous for the whole network. For these conditions, UAVs themselves account for the correction, and if UAVs fail to confirm the PoR, each UAV selects its own PoR from the available list and shares its coordinates. Here, the secondary Petri nets model of the underlying infrastructure is of extreme importance. Once the Petri nets are validated for every UAV, and all the UAVs have obtained the required data during the one timestamp, every UAV starts calculating its flying coordinates by building the maps from the context shared between each vehicle and the underlying infrastructure.

3D Maps from Petri Nets

The proposed approach does not fall into complex mapping for generating non-overlapping coordinates; rather, the proposed approach takes into account the coordinates along with the height and area to generate a 3D cylinder that encircles the entire building. This simple approach also reduces the number of complex computations for generating graphical maps on the UAVs. The provided solution supports all types of UAVs irrespective of the degree of manoeuvrability. O_b acts as a decisive metric for generation of non-overlapping waypoints, as shown in the entire approach in Fig. 3. The two parts of the figure show the actual urban scenario (Fig.



P0	Mission_Input
P1	Command to airborne
P2	PoR selection
P3	Notify PoR
P4	Share PoR info
P5	Advertise & Ack
P6	Operational decision
P7	Map construction
P8	Coordinate evaluation
P9	Adjacent drones
P10	Area/height (AP/PoR)
P11	Correctness of PoR

T0	Beaconing
T1	PoR request
T2	PoR context
T3	Share PoR context
T4	Transmit coordinate
T5	PoR decision
T6	Maneuver coordinates
T7	Shared entity
T8	Correctness of area

C1	<Uid>
C2	<Uid, (x,y,z), Θ>
C3	<Uid, (x,y,z), Θ, τ>
C4	<Uid, (x,y,z), Θ, τ, Rid>
C5	<Uid, (x,y,z), Θ, τ , Rid, Lid>
C6	<Uid, τ, Rid, Lid, Aid>
C7, C8	<Uid, Lid, Θ, τ>
C9	<Uid, Lid, Θ, τ, A, H>
C10,C11	<Uid, (x,y,z), Θ>
C12,C13	<Lid, Pα, Pη, τ>
C14,C15	<Pα, Pη, τ>
C16,C17	<Uid, Lid, Θ, τ, A, H, Ob>
C18	<Uid, (x,y,z), Θ, Ob>
C19,C20	<Uid, (x,y,z), Θ, τ, (x,y,z)', Ob>
C21	<Uid, Lid, Aid, α, τ>
C22	<Uid, Ack>
C23,C24	<Uid, α>
C25	<Uid, Lid, (x,y,z)', α, Θ, A, H>
C26	<Lid, τ>
C27,C28	<Uid, Lid, (x,y,z)', α, Θ, τ, A, H>

P'0	PoR
P'1	Next PoR
P'2	Selected UAVs
P'3	Coordinate info
P'4	Other UAVs to LFR
P'5	Validate coordinates
P'6	Decision/update

T'0	Context share
T'1	Advertise-UAVs
T'2	Share coordinates
T'3	Validate context
T'4	Transfer list of UAVs
T'5	Validate coordinates

C'1,C'2,C'3	<Lid, (x,y,z), A, H, Uids, m>
C'5	<Lid, (x,y,z)', Uids, m>
C'4,C'6	<Lid, Uid, τ, Θ)>
C'7	<Lid, m, Uid, (x,y,z), A, H>
C'8,C'9	∀<Lid, m, Uid, A, H>
C'10,C'11	∀<Lid, m, Uid, (x,y,z)>
C'12,C'13	<Lid, Uid, (x,y,z)>
C'14	<Uid, m, Θ, A, H>
C'15,C'16	∀<Lid, m, Uid, (x,y,z), Θ, τ, A, H>

Figure 2. Context-awareness for drones using hierarchical aspect-oriented Petri nets: a) context-aware aspect-oriented Petri nets for UAV cooperation; b) aspect-oriented Petri nets for underlying infrastructure; c) hierarchical and dynamic context-aware aspect-oriented Petri nets for infrastructure-assisted localization of drones in an urban scenario.

All the entities operate over a secure channel and, a pre-established trust is assumed between them, which is set during the initial configuration of the network. This protocol provides a strategy for attaining context from any active entity in the network, and the security of context is validated by using the hierarchical aspect-oriented Petri nets.

Once the UAV acknowledges the attachment ID along with its context, the PoR pushes a group key to all the flying vehicles. This push key [15] is used for communication between the multiple UAVs. The context between the UAVs is protected by Hash Message Authentication Code (HMAC) based on group key.

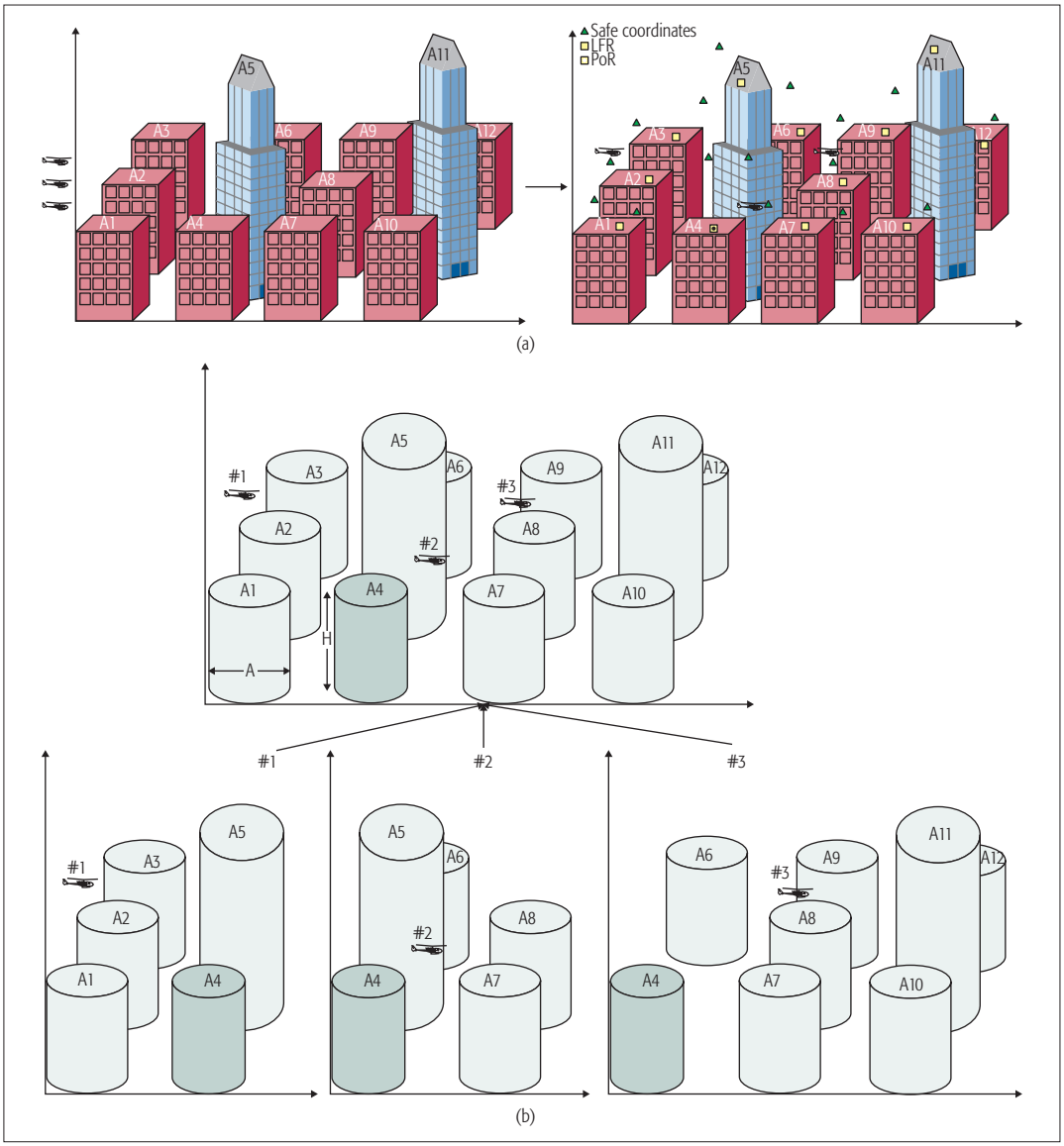


Figure 3. Context-aware 3D maps for drones using hierarchical aspect-oriented Petri nets: a) actual urban scenario for drone localization; b) scenario divisibility and localization map formation for drones using hierarchical context-aware aspect-oriented Petri nets.

3a) and the 3D-cylindrical image plotted by the drones (Fig. 3b). The data for the entire solution is observable from PoR. Thus, security of PoR is the key, and the updating of PoR after a certain timestamp helps in reducing the risk of vulnerability. The flowchart in Fig. 4a gives the procedures for coordinating the UAVs and generating 3D maps. The procedures operate with a complexity of $O(m)$, where m is the number of UAVs deployed in the urban scenarios. Every step in the flowchart accounts for onboard processing on the UAVs. This requires sufficient energy to keep the system operational. Since UAVs are powered by batteries, the procedures should not consume excessive energy resources, and the validation should be less burdened.[2]

Protocol for Securing Context of Drones

The proposed approach uses a secure communication channel that helps in disseminating the context via security validations over the Petri nets. Figure 4b illustrates the procedures for sharing the context between the UAVs in the urban scenarios. All the entities operate over a secure channel, and a pre-established trust is assumed between them, which is set during the initial configuration of the network. This protocol provides a strategy for attaining context from any active entity in the network, and the security of context is validated by using the hierarchical aspect-oriented Petri nets. Availability of LoS facilitates the U2U communication. Each fixed entity and the selected PoR always beacon availability messages to the UAVs over the assumed secure channel.

The path between the UAVs and the PoR is assumed to be secured by a pre-established trust through Advanced Encryption Standard (AES). The context transfer begins with an attachment request followed by a new U_{id} allotted to the requesting UAV by the PoR. Every PoR maintains its own list of allocated IDs and always uses separate IDs for communication with different UAVs. UAVs always advertise their generic IDs, which are allotted during mission configurations. Once the UAV acknowledg-

[2] Currently, energy constraints are not considered in the proposed approach.

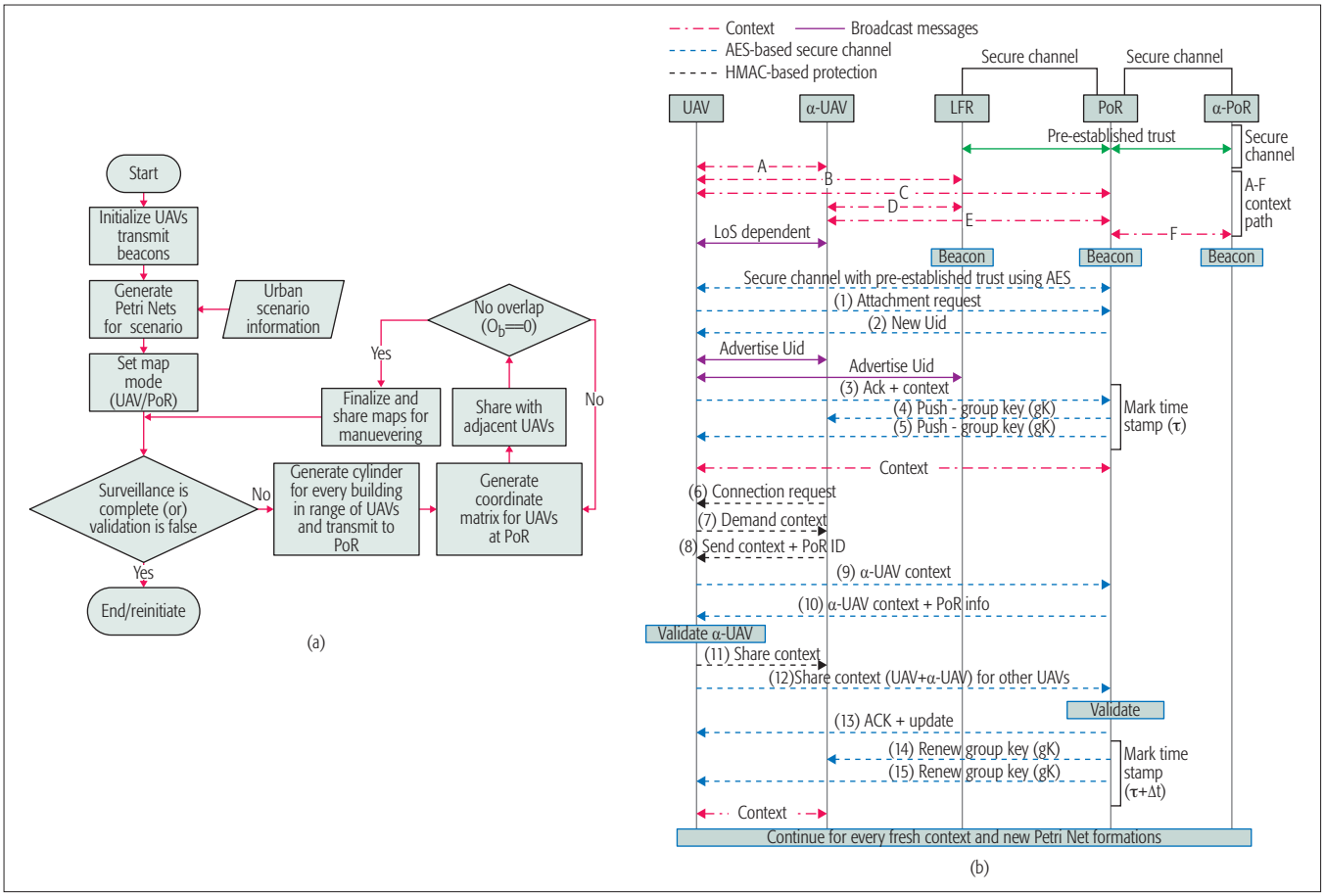


Figure 4. a) Flowchart for generation of context-aware 3D maps from Petri nets; b) protocol for secure context sharing over generated Petri nets between the urban entities. α denotes the adjacency.

es the attachment ID along with its context, the PoR pushes a group key to all the flying vehicles. This push key [15] is used for communication between the multiple UAVs. The context between the UAVs is protected by Hash Message Authentication Code (HMAC) based on a group key.

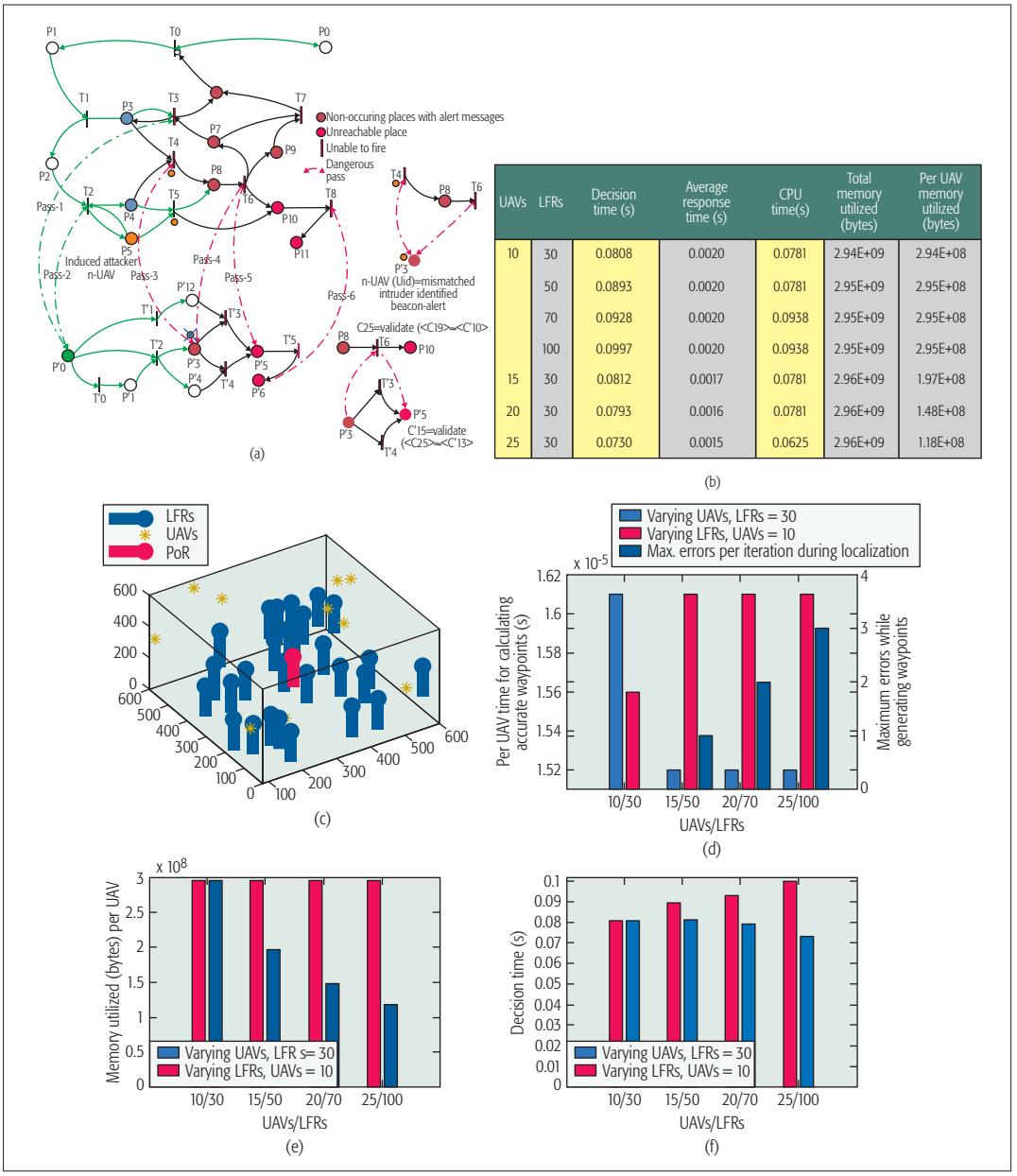
Once a UAV (α – UAV) makes a connection request to another UAV (to establish a U2U network), the requested UAV demands the context for location awareness. On receiving, it transfers the context to PoR, which sends the pre-validation results along with its details to the requesting UAV. Here, the PoR acts as a third party and checks the context in its list and validates with its own Petri nets model. The requested UAV compares it with the context from PoR and shares its own context after validating the information. For further security, the requested UAV again transfers the shared context to PoR, which validates with acknowledgment and update message. Next, the PoR renews the group keys. This re-validation is only performed in extreme-attacker scenarios. The proposed approach provides a strong U2U context exchange mechanism, but the success depends only on the secure validation of background Petri nets.

Case Study and Performance Evaluation

The security of the coordinates for drones in the urban scenario depends on their interaction with each other and the LFRs. This case study helps to analyze the security of the proposed system and to validate the hierarchical aspect-oriented Petri nets for secure drone localization. An attacker is induced in the form of a UAV that tries to locate the other UAVs and provide false data which hinders cooperative movement and may result in loss of other UAVs.

The case study follows the hierarchical context-aware aspect-oriented Petri nets presented in Fig. 2c. Figure 5a illustrates the detailed validation procedure for drones. The passes in the Petri nets help in identification of the vulnerable context, which can be used by the attacker to modify the information of coordinates. In Fig. 5a, the intruder interacts at place P5 of the Petri nets model and fires transitions T5 and T2, but as it reaches *P'*3 via T6, the validation procedure (mismatch of the context) at this place identifies the potential threat and advertises it through the beacons over the secure channel. This is the dangerous pass, which leads to a potential conflict of context. Next, places P10 and P'5 perform the final validation by considering the context-exchange procedures as suggested in Fig. 4 as well as for the context obtained from the previous transition in the Petri nets, and finally eliminates the intruder by changing the PoR. Whenever a dangerous pass occurs, the places corresponding to it are unable to proceed with the next transition. This is the non-firing of transition, and the places following such transitions are the unreachable places. The proposed approach is capable of tracking the point where an intruder interacted with the other

The localization of UAVs deals with the setting of waypoints which can help in maneuvering without collision. If there are any errors in localization, there is a high probability of collision and the entire approach may fail. Thus, the proposed approach focuses on deriving correct waypoints which do not have any overlapping coordinates as well as are free from redundant paths.



UAVs	LFRs	Decision time (s)	Average response time (s)	CPU time(s)	Total memory utilized (bytes)	Per UAV memory utilized (bytes)
10	30	0.0808	0.0020	0.0781	2.94E+09	2.94E+08
	50	0.0893	0.0020	0.0781	2.95E+09	2.95E+08
	70	0.0928	0.0020	0.0938	2.95E+09	2.95E+08
	100	0.0997	0.0020	0.0938	2.95E+09	2.95E+08
15	30	0.0812	0.0017	0.0781	2.96E+09	1.97E+08
20	30	0.0793	0.0016	0.0781	2.96E+09	1.48E+08
25	30	0.0730	0.0015	0.0625	2.96E+09	1.18E+08

Figure 5. Case study and simulation results: a) an illustration of the validation procedure using the hierarchical context-aware aspect-oriented Petri nets for secure and efficient localization of multiple drones in an urban scenario; b) detailed results with varying number of UAVs and LFRs for different metrics; c) 3D view of the urban scenario as computed by the 10 UAVs with 30 LFRs and 1 PoR; d) errors due to overlapping waypoints and per UAV time consumption for accurate generating waypoints after each iteration; e) per UAV memory utilization vs. number of UAVs and LFRs; f) decision time for localization vs. number of UAVs and LFRs.

UAVs by tracing back to the last point that matches the context of the identified intruder.[3]

The localization of UAVs deals with the setting of waypoints, which can help in maneuvering without collision. If there are any errors in localization, there is a high probability of collision, and the entire approach may fail. Thus, the proposed approach focuses on deriving correct waypoints that do not have any overlapping coordinates and are free from redundant paths. Thus, the article includes results for the time required by the proposed approach to arrive at a decision of finalized waypoints for UAVs as well as errors in localization.

The proposed context-aware localization is evaluated for its performance in generating 3D waypoints-based maps of urban scenarios by UAVs ranging between 10 and 30. The number of buildings with LFRs varies between 30 and 100. A 10 MHz channel is set for all of the simulations, which are conducted in Matlab. Figure 5b gives the detailed results for various metrics. If the approach has to undergo many iterations for identifying accurate and non-overlapping waypoints, the decision time increases, which is not desirable for urban surveillance.

Currently, the context messages between UAVs are protected by HMAC using group key with Secure Hash Algorithm (SHA) of 160 bits. The proposed approach can be operated with varying HMAC, such as SHA-256 bits. AES (128 bits)

[3] Recovery and re-establishment phases are beyond the scope of this article.

Approaches/ parameters	Spatially secure group communication	PCA-based line detection for localization	Multi-UAV guided ground network formations	3D localization using indoor WiFi antennas	Proposed secure and context-aware localization
Author	Kim and Seo (2012)	Opromolla *et al.* (2017)	Sharma and Kumar (2015)	Flores *et al.* (2017)	Sharma *et al.*
Vehicle type	Unmanned autonomous vehicles (UAVs)	Unmanned aerial vehicles (UAVs)	Unmanned aerial vehicles (UAVs)	Unmanned aerial vehicles (UAVs)	Unmanned aerial vehicles (UAVs)
Security	Yes Spatial communication security	No	No	No	Yes Context-aware security
Outcome	Analytical framework for multiple UAVs and control from security perspective	Autonomous navigation of UAVs with 2D-LIDAR in GPS challenges scenarios	Cooperative network between UAVs and ground nodes for localization and positioning control	3D localization system using Angle of Arrival in combination with WiFi signals	Secure localization of UAVs in urban scenario with 3D mapping
Topology	Undirected graph with UAVs as vertices and transmission links as graphs	Line-based algorithm for autonomous positioning of UAVs	Octagonal topology with UAVs at octagons centers and ground nodes at squares	Autonomous planning around objects by using WiFi signals for UAVs	Adaptive and autonomous maneuvers around urban buildings using LFRs and PoR
Key tasks	Cooperative UAV control; Transmission power control; Position interference; Routing and Scheduling	Line-based mapping of environment; and UAV localization	Cognitive maps for UAVs, nodes, and area; and waypoints generation for non-redundant search	Router-assisted network formation to transmit sensing information and RSSI to UAVs	3D map formations of urban scenario; location identification of buildings and UAVs; security of coordinate exchange;
3D visualization	No	Partial	No	No	Yes
Localization	Yes	Yes	Yes	Yes	Yes
Securing U2U context	No	No	No	No	Yes
Scenario type	Wireless scenario with spatial reuse	3D to 2D maze-based environment	Wireless scenario with links between UAVs and ground nodes	Smart indoor scenario with WiFi capacity	3D urban scenario with support from underlying wireless network

Table 1. State-of-the-art comparison between the proposed approach and key solutions for the localization of UAVs.

protects the channel between the UAVs and the PoR, and also secures the push key. These keys can be changed on the basis of the applied algorithm. However, the trade-off between the performance and the selection of appropriate key size should be handled, and this will vary for different scenarios. Apart from this, adaptive or dynamic adjusting key solutions can give better performance in the considered scenario. The key size affects the context burden of the network and should be carefully selected. The numerical simulations show the standard context-based message size is between 1248 B (except for incidence matrix) and 14,048 B (for all operations), which lowers to 368 bytes if only LFRs provide the location of neighbors and distance updates. The number of entities and configurations of the entire urban scenario affect the context size. The total memory used per UAV during the entire process is between 1.18E+08 and 2.94E+08 bytes.

Figure 5c illustrates a 3D graph view for 10 UAVs in an urban scenario with 30 LFRs and 1 PoR. This graph demonstrates the non-overlapping and collision-free context-based map generation of an urban environment. Figure 5d shows the results for errors in localization. The graph presents the per iteration time consumption for each UAV while generating accurate waypoints, and suggests that the maximum errors are within the range of 3 percent, which is correctable even in adverse attacker conditions. Results in Fig. 5e show that the memory consumption is not much affected by the variation in the number of LFRs; however, per-UAV memory consumption decreases with an increase in the number of UAVs at a fixed number of LFRs as there is sharing of context between the vehicles, and each has to store less information. Also, the decision time (Fig.5f), including the validation procedures and U2U agreements, increases with an increase in the number of LFRs at constant UAVs as more computations (validations as well as authentications) are to be performed for each UAV, and decreases with an increase in the number of UAVs with fixed LFRs as the number of validations decreases in comparison to the prior scenario.

State-of-the-Art Comparison

With the increasing demand for UAVs in the next generation of networks, the localization of UAVs in the urban scenario is a crucial issue to resolve. Along with localization, security of UAVs as well as types of environments are of central importance. However, most of the existing solutions focus on either security or localization — none have addressed both these requirements jointly. A state-of-the-art comparison (Table 1) is drawn with some of the key solutions that prove the effectiveness as well as the reach of the proposed solution in providing 3D context-aware and secure localization of UAVs in urban scenarios.

Concluding Remarks and Future Directions

Localization of drones in urban environments demands high precision and accuracy in the selection of waypoints and hovering data so as to prevent any collision. The cooperation between

The cooperation between multiple drones facilitates urban surveillance and in combination with powerful solutions such as cooperative map building and cooperative task resolutions, it can help in visualizing the urban scenario in 3D. The success of efficient localization depends on the type of context and secure context sharing between the aerial vehicles.

multiple drones facilitates urban surveillance and, in combination with powerful solutions such as cooperative map building and cooperative task resolutions, it can help in visualizing the urban scenario in 3D. The success of efficient localization depends on the type of context and secure context sharing between the aerial vehicles. This article demonstrates a novel solution that is capable of securing the context information for sharing 3D maps between the UAVs. Also, the proposed approach provides a secure path for U2U collaboration and context validation by using hierarchical aspect-oriented Petri nets.

There are certain key aspects that are yet to be resolved in this area of research. These include:

- Embedded security for the onboard components is a significant challenge to be overcome.
- Integrating drones with modern types of cellular equipment such as cloud radio access networks or several backhaul units is a major issue.
- Resolution of context transfer and handoffs between multiple drones and the underlying infrastructure is still an open issue.
- Strict evolution of security approaches for different attacker conditions must be ensured.
- Pattern imaging and machine learning solutions can be applied to identify possible intruders during urban surveillance.

Acknowledgment

This work was partly supported by an Institute for Information & Communications Technology Promotiongrant funded by the Korean government (MSIT) (No.2017-0-00664, Rule Specification Based Misbehavior Detection for IoT-Embedded Cyber Physical Systems) and the Soonchunhyang University Research Fund. Dr. Ilsun You is the corresponding author.

References

[1] Z. M. Fadlullah *et al.*, "A Dynamic Trajectory Control Algorithm for Improving the Communication Throughput and Delay in Uavaided Networks," *IEEE Network*, vol. 30, no. 1, Jan./Feb. 2016, pp. 100–05.
[2] D. Wu *et al.*, "Addsen: Adaptive Data Processing and Dissemination for Drone Swarms in Urban Sensing," *IEEE Trans. Computers*, vol. 66, no. 2, 2017, pp. 183–98.
[3] I. Maza *et al.*, "Experimental Results in Multi-UAV Coordination for Disaster Management and Civil Security Applications," *J. Intelligent & Robotic Systems*, vol. 61, no. 1, 2011, pp. 563–85.
[4] X. Wang *et al.*, "Cooperative Target Localization Using Multiple UAVs with Out-of-Sequence Measurements," *Aircraft Engineering and Aerospace Technology*, vol. 89, no. 1, 2017, pp. 112–19.
[5] A. Orsino *et al.*, "Effects of Heterogeneous Mobility on D2D and Drone-Assisted Mission-Critical MTC in 5G," *IEEE Commun. Mag.*, vol. 55, no. 2, Feb. 2017, pp. 79–87.
[6] P. Ladosz, H. Oh, and W.-H. Chen, "Trajectory Planning for Communication Relay Unmanned Aerial Vehicles in Urban Dynamic Environments," *J. Intelligent & Robotic Systems*, 2017, pp. 1–19. DOI:10.1007/s10846-017-0484-y.
[7] P. Wang *et al.*, "Offline Perching Location Selection for Quadrotor UAV in Urban Environment," *12th IEEE Int'l. Conf. Control and Automation*, Kathmandu, Nepal, 2016, pp. 1008–13.
[8] C. Constantinides and P. Parkinson, "Security Challenges in UAV Development," *27th IEEE Digital Avionics Systems Conf.*, MN, 2008, pp. 1–8.
[9] S.-W. Kim and S.-W. Seo, "Cooperative Unmanned Autonomous Vehicle Control for Spatially Secure Group Communications," *IEEE JSAC*, vol. 30, no. 5, 2012, pp. 870–82.
[10] R. Opromolla *et al.*, "PCA-Based Line Detection from Range Data for Mapping and localization-Aiding of UAVs," *Int'l. J. Aerospace Engineering*, vol. 17, 2017, pp. 1–14. DOI. org/10.1155/2017/4241651.
[11] V. Sharma and R. Kumar, "A Cooperative Network Framework for Multi-UAV Guided Ground Ad Hoc Networks," *J. Intelligent & Robotic Systems*, vol. 77, no. 3–4, 2015, pp. 629–52.
[12] D. Flores, D. Marcillo, and J. Pereira, "3D Localization System for an Unmanned Mini Quadcopter Based on Smart Indoor Wi-Fi Antennas," *World Conf. Info. Systems and Technologies, Advances in Intelligent Systems and Computing*, Springer, vol. 571, 2017, pp. 543–50. DOI: 10.1007/978-3-319-56541-5_55.
[13] T. Murata, "Petri Nets: Properties, Analysis and Applications," *Proc. IEEE*, vol. 77, no. 4, 1989, pp. 541–80.
[14] D. Xu and K. E. Nygard, "Threat-Driven Modeling and Verification of Secure Software Using Aspect-Oriented Petri Nets," *IEEE Trans. Software Engineering*, vol. 32, no. 4, 2006, pp. 265–78.
[15] F. Sato and S.-Y. Tanaka, "A Push-Based Key Distribution and Rekeying Protocol for Secure Multicasting," *Proc. 8th Int'l. Conf. Parallel and Distributed Systems*, Kyongju City, South Korea, 2001, pp. 214–19.

Biographies

Vishal Sharma [S'13, M'17] (vishal_sharma2012@hotmail.com) received his Ph.D. and B.Tech. degrees in computer science and engineering from Thapar University (2016) and Punjab Technical University (2012), respectively. He worked at Thapar University as a lecturer from April 2016 to October 2016. He was a postdoctoral researcher at Soongsil University and Soonchunhyang University, South Korea, from November 2016 to September 2017. Now, he is a research assistant professor at the Department of Information Security Engineering, Soonchunhyang University, Republic of Korea.

Dushantha Nalin K. Jayakody [M'14] (nalin.jayakody@ieee.org) received his M.Sc. degree in electronics and communications engineering from Eastern Mediterranean University, Cyprus. He received his Ph. D. degree in electronics and communications engineering from University College Dublin, and held postdoctoral positions (2014–2016) at the University of Tartu and the University of Bergen. Now, he is an associate professor at the Institute of Cybernetics, National Research Tomsk Polytechnic University.

Ilsun You [SM'13] (ilsunu@gmail.com) received his M.S. and Ph.D. degrees in computer science from Dankook University, Korea, in 1997 and 2002, respectively. He received his second Ph.D. degree from Kyushu University, Japan, in 2012. From 1997 to 2004, he was at THIN Multimedia, Internet Security, and Hanjo Engineering as a research engineer. Now, he is an associate professor at the Department of Information Security, Soonchunhyang University. He is a Fellow of IET.

Ravinder Kumar [M'17] (ravinder@thapar.edu) received his Ph.D. degree in computer science and engineering from Thapar University in 2015. He is currently an assistant professor in the Computer Science and Engineering Department, Thapar University. His area of research includes theoretical and practical aspects of combinatorial optimization, approximation algorithms, and mathematical programming.

Jun Li [M'09, SM'16] (jun.li@njust.edu.cn) received his Ph.D. degree in electronic engineering from Shanghai Jiao Tong University, P. R. China, in 2009. He was a research scientist (2009) at Alcatel Lucent Shanghai Bell, a postdoctoral fellow (2009–2012) at the University of New South Wales, Australia, and a research fellow (2012–2015) at the University of Sydney, Australia. Since June 2015, he has been a professor at the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, China.