Journal of Cybersecurity and Privacy

MDPI

*Article*

# Trustworthiness of Situational Awareness: Significance and Quantification

**Arslan Munir [1,*], Alexander Aved [2], Khanh Pham [3] and Joonho Kong [4]**

[1] Department of Computer Science, Kansas State University, Manhattan, KS 66506, USA
[2] Air Force Research Laboratory, Information Directorate, Rome, NY 13441, USA; alexander.aved@us.af.mil
[3] Air Force Research Laboratory, Space Vehicles Directorate, Albuquerque, NM 87117, USA; khanh.pham.1@spaceforce.mil
[4] School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, Republic of Korea; joonho.kong@knu.ac.kr
* Correspondence: amunir@ksu.edu

**Abstract:** Situational awareness (SA) is of tremendous significance for successful operations in many domains, such as surveillance, humanitarian, search, and rescue missions, and national security. SA is particularly important for the defense sector, and is regarded as the decisive factor in military and air combat engagements. Commanders and operators rely on the accuracy and fidelity of SA for comprehending the environment, decision-making, and carrying out actions based on these decisions for accomplishing a mission. SA, however, is susceptible to adversarial attacks that can compromise the security and trust of SA systems. In this paper, we discuss the significance of security and trust of SA from an air force perspective. We then propose a model for quantifying the trustworthiness of an SA system. We further present numerical examples that demonstrate the quantification of trustworthiness of an SA system using our proposed model. Finally, we conclude this paper with future research directions for quantifying the security of SA systems.

**Keywords:** situational awareness; security; integrity; trustworthiness; common operating picture; modeling



**Citation:** Munir, A.; Aved, A.; Pham, K.; Kong, J. Trustworthiness of Situational Awareness: Significance and Quantification. *J. Cybersecur. Priv.* **2024**, *4*, 223–240. https://doi.org/10.3390/jcp4020011

Academic Editor: Danda B. Rawat

Received: 5 December 2023
Revised: 10 February 2024
Accepted: 22 March 2024
Published: 8 April 2024



## 1. Introduction

Situational awareness (SA) is the perception of entities in an environment, the comprehension and interpretation of their meaning, and the projection or prediction of their status in the near future. From an air force perspective, SA means the capability of understanding the current and future disposition or status of red and blue aircraft and surface threats within a volume of space [1].

SA is of a tremendous significance for military and air forces, and is considered as the decisive factor in military and air combat engagements [2,3]. The United States Air Force (USAF) war theorist Colonel John Boyd [4] considered SA as analogous to the "observe" and "orient" stages of the observe–orient–decide–act (OODA) loop. SA is also an integral component of military command and control (C2). The C2 is comprised of SA, planning, tasking, and control. The C2 system design is intended to present the situation to the commander in a way that promotes the accurate and comprehensive understanding of the situation so that the best action can be taken.

Figure 1 provides an overview of an SA system from an air force perspective. Figure 1 shows the sources that are typically employed in a military and/or air force to obtain SA. These sources include short-range and long-range intelligence, surveillance, and reconnaissance (ISR) UAVs, fighter and reconnaissance aircraft, satellites, radars, heads-up displays (HUDs), helmet-mounted displays (HMDs), and different types of sensors, such as gunshot detectors and locators, microphones, audio recorders, smoke/fire detectors, and motion sensors. The sources of information for providing SA can be categorized as

human intelligence (HUMINT), measurement and signature intelligence (MASINT), imagery intelligence (IMINT), open source intelligence (OSINT), signals intelligence (SIGINT), and geospatial intelligence (GEOINT). HUMINT is a type of intelligence derived from information acquired and provided by human sources. MASINT refers to the intelligence obtained by acquiring and measuring the intrinsic characteristics and components of an object or activity via sensing instruments that enable the object or activity to be detected, recognized, or characterized every time it is encountered. MASINT includes radar intelligence, acoustic intelligence, nuclear intelligence, and chemical and biological intelligence. In IMINT, imagery is analyzed to infer information of intelligence value. For defense intelligence purposes, imagery that is typically utilized is acquired by satellite or aerial photography through ISR UAVs or aircraft. OSINT refers to the type of intelligence that is obtained from capturing and analyzing publicly available information, such as news media, public records, social media platforms, and websites, etc. SIGINT is a type of intelligence derived from the interception and collection of information from various electronic signals and systems, such as communications systems (including decoding encrypted messages), radars, and weapons systems, and is often used to obtain insight into the modus operandi of an adversary or target. GEOINT refers to the type of intelligence that exploits and analyzes imagery and geospatial information to assess and visually depict physical features and geographically referenced activities on Earth. GEOINT comprises imagery, IMINT, and geospatial information. Information gathered from these different intelligence sources is fused with the help of data fusion systems (e.g., radar data fusion, aircraft data fusion, UAV data fusion), and is then passed to a common operating picture (COP) builder computer, which engenders a COP or user-defined operating picture (UDOP), which is an evolution of the COP.

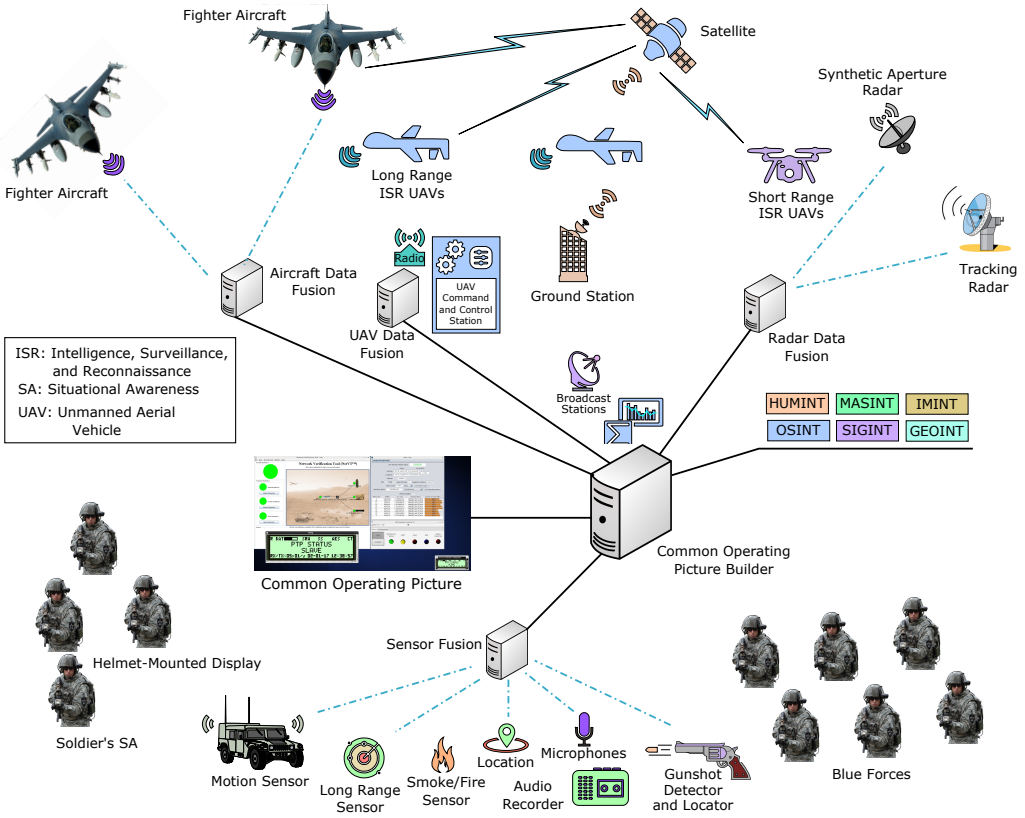


**Figure 1.** Overview of situational awareness [1].

The SA devices are integral for obtaining perception and comprehension of an environment; however, SA devices and an SA system are vulnerable to adversarial attacks that can jeopardize the security and trust of SA systems. These attacks encompass both passive and active attacks that target the sensors, communication links, electronics, and artificial

intelligence (AI) of SA devices, equipment, and systems [3] as further discussed in Section 3. To protect SA devices and systems against these security attacks and to impart trust in these SA systems, mitigation techniques need to be incorporated to alleviate these security attacks on SA. This paper contemplates security and trust issues in SA and proposes a model for quantifying the trustworthiness of an SA system. To the best of the authors' knowledge, the proposed model is the first of its kind to quantify the trustworthiness of SA systems. The proposed model is a simple yet practical model, that enables efficient estimation of trustworthiness for different SA sources. Our main contributions in this paper are as follows:

- We discuss the significance of security and trust in SA systems from a military and an air force perspective;
- We elaborate the significance of quantifying the trustworthiness of SA systems for improving the trust of SA systems;
- We propose a model for quantifying the trustworthiness of an SA system;
- We present numerical examples that demonstrate the quantification of the trustworthiness of an SA system using our proposed model.

To the best of the authors' knowledge, this is the first paper that targets the quantification of the trustworthiness of SA, and can serve as a guideline for future research in this area. The remainder of this paper is organized as follows. Section 2 provides a summary of relevant works in the literature related to the assessment and security of SA. Section 3 discusses the security and trust of SA and identifies the different components of an SA system that can be subjected to adversarial attacks. Section 4 illustrates the significance of quantifying the integrity of SA on the trust of SA systems and also presents our proposed model for quantifying the trustworthiness of an SA system. Section 5 shows numerical results and examples of the trustworthiness quantification of the SA system. Finally, Section 6 concludes this paper.

## 2. Related Work

Many works in the literature have explored SA. Endsley [5] has presented a theoretical model for SA considering its role in human decision-making. According to the Endsley's model, SA consists of three levels, where the first level pertains to the perception of elements in the current situation, the second level means the comprehension and interpretation of the current situation, and the third level refers to the projection and prediction of the future status of entities in the environment, at least in the near term. Munir et al. [1] have enhanced Endsley's model to incorporate AI and dynamic data-driven application systems to adapt measurements and resources in accordance with changing situations. They have also discussed the measurement of SA and the challenges associated with the quantification of SA. They have also elaborated technologies that could improve SA, ranging from different means of intelligence gathering to AI to automated vision systems.

Establishing metrics to quantify the performance of SA is very crucial for SA system design. Some of the metrics for SA assessment include [1]: (i) timeliness, (ii) accuracy, (iii) trust, (iv) credibility (can be characterized by a confusion matrix of probability of detection and probability of false alarm), (v) availability, (vi) cost, (vii) attention, (viii) performance (success in completing the mission and to evaluate decisions taken), and (ix) scope (local versus global or single-intelligence (single-INT) versus multi-intelligence (multi-INT)). These metrics can be used for design as well as to assess the SA by quantitatively evaluating various aspects of the SA.

An SA measurement approach should include a variety of system design concepts, including [6]: (i) display symbolism, such as 3D displays, voice control, flat panel displays, HUDs, and HMD, etc.; (ii) electronics, avionics, and sensing concepts; (iii) information fusion concepts; (iv) automation; (v) integrity; (vi) trustworthiness; and (vii) training techniques. Nguyen et al. [7] have discussed different SA assessment approaches, which use different types of probes to measure SA, such as freeze-probe techniques, real-time probe techniques, post-trial self-rating techniques, observer-rating techniques, performance-

based rating techniques, and process indices-based rating techniques. These techniques can be used in many real-world applications. SA measurement techniques that are often utilized include (i) NASA task load index (TLX) (please note that it could also be utilized to assess situational awareness in cognitive workloads) [8], (ii) SA global assessment technique (SAGAT) [6], (iii) SA rating technique (SART) [9], and (iv) critical decision method (CDM) [10]. A rigorous summary of these techniques is presented in [1], and is omitted here for brevity.

SA can be measured by empirically assessing an operator's performance via quantifiable metrics, such as time and accuracy, and then by comparing these assessments to the results of similar tests without SA assistance. However, little work exists on quantifying SA [11]. Furthermore, most of the existing methods for measuring SA have various shortcomings, such as subjectivity [12], physiology [13], limitedness [11], and coverage. Different metrics have been proposed to assess the worthiness of an SA system. These metrics can be characterized into five categories or dimensions [11]: (i) confidence, (ii) accuracy/purity, (iii) timeliness, (iv) throughput, and (v) cost.

Although many works have discussed SA and SA assessment techniques, the security of SA has not been explored in the literature. The most relevant work related to the security of SA is [3], where the authors discussed the security and trust issues in SA, and contemplated various passive and active adversarial attacks on SA systems. The authors further presented different approaches for mitigating adversarial attacks on SA, such as robustness against transduction attacks, symmetric and asymmetric cryptography, hardware-based security, and AI security. However, the work did not present any model for quantifying the trustworthiness of an SA system. This work aims to fill in the gap in the literature pertaining to the security of SA and presents a model for the first time to quantify the trustworthiness of SA.

## 3. Security and Trust of Situational Awareness

This section elaborates the significance of the security of and trust in SA from an air force perspective. This section first discusses the security and trust issues of a COP presented to the commander. The section then discusses the SA components in an SA system susceptible to attacks, followed by the impacts of security attacks on COP.

### *3.1. Security of Common Operating Picture (COP)*

COP is used to display SA to commanders. UDOP is an evolution of of COP, which makes it possible to dynamically present an operator's or commander's view of the information. The COP is generally a display shared by more than one command teams, where each command team is in control of their operating picture. The availability of COP helps mission command by enabling all the participants to see the overall operation and their contributions to it as the operation proceeds [14]. The COP information is obtained from various sources as shown in Figure 1. The COP also includes situation reports, which are compiled by a commander's line staff, based on their comprehension of available information. However, SA is susceptible to security attacks, and the trustworthiness of COP can be negatively effected by faults (in sensors, hardware, and software), security attacks, and/or misprojection of information.

### *3.2. SA Components Susceptible to Security Attacks*

Figure 2 shows potential security attacks on different SA components that can negatively affect the integrity and trust of COP. Mainly, the security attacks can be characterized by four main aspects of SA:

- Attacks on communication links;
- Attacks on sensors;
- Attacks on the computing hardware of SA infrastructure; and
- Attacks on the equipment of dismounted operators and pilots.

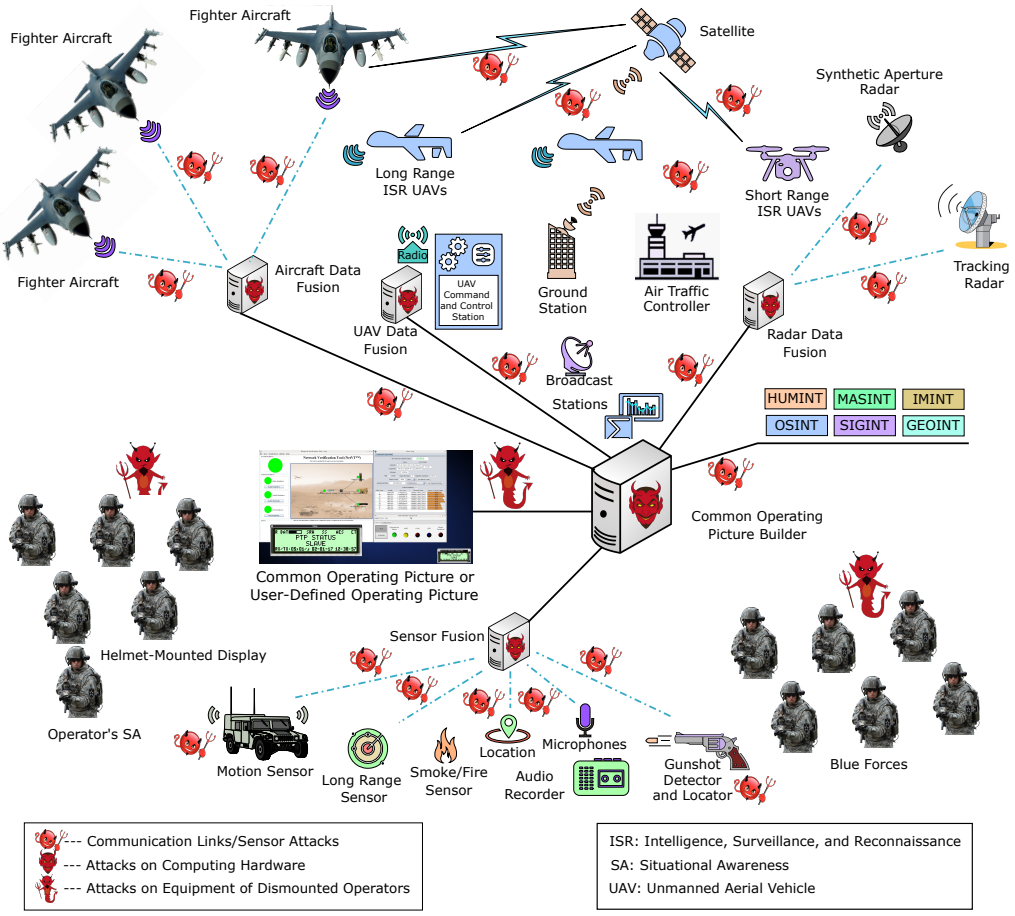


**Figure 2.** Security issues in situational awareness [3].

Both the wired and wireless communication links are vulnerable to security attacks. As depicted in Figure 2, it is possible for an attacker to compromise the communication links between: (i) radars and the radar data fusion center, (ii) satellite and UAVs, (iii) satellites and fighter aircraft, (iv) aircraft and the aircraft data fusion center, (v) the ground station and the UAVs, (vi) sensors and the sensor fusion center, (vii) the sensor fusion center and the COP builder, (viii) the radar data fusion center and the COP builder, (ix) the UAV data fusion center and the COP builder, (x) the aircraft data fusion center and the COP builder, (xi) the COP builder and the commander's COP display center, and (xii) the COP builder station and other recipients of COP. Sensors can be attacked to manipulate the physical properties of sensors to provide malicious readings [15]. An attacker can also conduct security attacks on the computing hardware of SA infrastructure including the radar data fusion center, aircraft data fusion center, sensor fusion center, UAV command and control station, and the COP builder. Finally, an attacker can compromise sensors and equipment, such as HUDs and HMDs, that are carried by dismounted operators and pilots.

### *3.3. Impacts of Security Attacks on COP*

Since different aspects of SA are susceptible to attacks, it is possible that the situation reports collected and compiled by a commander's line staff, and the SA acquired by the COP builder are subjective, inaccurate, and compromised. For a trustworthy COP, it is imperative to have consistency in the measurements, methods, and values within the COP. For example, let us see the effect of security attacks on SA and COP for a compromised link. If one of the links to the COP, such as aircraft positions and flight paths, becomes broken or compromised, it can affect the following factors regarding the COP and the commander's SA [14]:

1. If the *COP displays the last available aircraft positions and flight paths*, the COP will not be accurate anymore. In this case, the commander is able to notice the failure of the communication link, and he/she will realize there are aircraft whose positions and paths are not current in the COP, but can impact the operation. If the commander is not able to discern that the link is down (i.e., not available), he/she will keep on trusting the displayed COP as real-time information;
2. If the *COP erases the last available aircraft positions and flight paths*, then the COP will not be accurate anymore. In this case, the commander will not be certain whether there are actually no aircraft in the region of interest or whether no aircraft are shown in the COP because the link is down.

In the case of link failure, the commander may envisage a few questions [14]:

1. Is the link down because of sabotage, attack, interference, or benign failure?
2. In cases where the link was sabotaged, what is the purpose behind that and which enemy force is responsible?
3. Can the data be trusted if the link becomes live again?
4. Will he/she be notified that the link is down?

From this example, we can see that the commander may be preoccupied with the above questions rather than focusing on the C2 operation. If the COP cannot be trusted, it can affect the commander's ability to make appropriate decisions, which can impact the result of the warfare and the safety of the troops and first responders. It has been observed that a commander either chooses to trust the COP or completely disregards it [14]. It is possible that, due to a single compromised element (e.g., sensor, equipment), the COP is not 100% accurate, but because it affects the trustworthiness of the COP, the commander may discard the entire COP as untrustworthy. This results in accurate inputs to the COP being unnecessarily ignored, which negatively impacts SA.

Since security attacks on SA can have serious consequences, defending against these security attacks is of tremendous significance to maintaining the trust and integrity of SA and COP. To assure that the SA acquired by the commander is trustworthy, security primitives need to be integrated in SA system design [3]. Furthermore, if the information is gathered remotely through a multitude of sensors and sources, the integrity of the data links becomes critical to providing trustworthy SA. Also, computing systems responsible for information fusion and COP generation need to be secure and trustworthy for obtaining a trustworthy SA. As it has been observed that commanders tend to totally disregard the COP when there are integrity issues in the COP, quantifying the integrity of SA and COP can help restore the trust of commander in the COP and thus help improve SA.

## 4. Quantifying Trustworthiness of SA

As discussed in Section 3, inaccuracy, incompleteness, and untrustworthiness of COP can adversely impact a commander's SA and C2 operation. Hence, to restore a commander's trust in SA and COP, it is worth quantifying the trustworthiness of SA and COP. Discussion of different approaches for incorporating security and trust in devices, links, and computing systems providing SA is beyond the scope of this paper (interested readers can refer to [3] for a summary of these approaches). Different SA devices and systems integrate different levels of security primitives because of cost and feasibility constraints. Thus, overall trustworthiness estimation of COP and perceived SA need to consider the complex organization of heterogeneous devices with different integrities that are connected with various communication links with different integrity levels. This section presents a model for quantifying the trustworthiness of COP and SA.

### *4.1. Model for Quantifying the Trustworthiness of COP*

Information sources providing SA and making up COP have metrics of precision, quality, and usability; however, these measures are not adequate for quantifying the integrity of SA. The SA system in charge of producing COP can apply information security principles along with hardware security primitives to the information and communications

technology (ICT) links and information sources. These information security principles include confidentiality, integrity, availability, authentication, and non-repudiation [16]. These information security principles can be incorporated either through traditional cryptography, hardware-based security primitives, or AI security primitives [3].

The trustworthiness of an information source or link can be assessed through information security principles, such as confidentiality, integrity, availability, authenticity, and non-repudiation. We briefly discuss these principles in the context of COP. The *confidentiality* of COP means that the information displayed on the COP is private and the red forces are not privy to the same information. The confidentiality of COP can be determined by inspecting the way in which information was received, that is, whether the information was received over insecure public network infrastructure or through private encrypted networks or through word-of-mouth or intelligence agencies. Hence, a relative confidentiality measure can be assigned based on the way information was received into the COP, which can then be used in the calculation of the integrity of the COP. The *integrity* of the information pertains to how intact the information is. For example, if the information is transmitted via a digital medium that included error checking and/or message authentication codes, the integrity can be regarded as high. The *availability* of the information means that the information source is available and not down. If the information is received at the required rate as and when expected, the availability of the source can be regarded as high. The *authenticity* pertains to the legitimacy of the information source. If the information source is authenticated by appropriate authentication mechanisms [16], its authenticity can be regarded as high. *Non-repudiation* refers to the security property where the sender of the information cannot deny the creation of the message. Since the commander makes decisions based on the information displayed on COP, the commander needs to know if the information sources will stand by the information they have provided, and the sources have provided the information after due diligence. Non-repudiation can have real implications in life and death situations. For instance, if the commander orders an air strike with the assurance that no friendly forces are present in the strike zone, he/she must have the confidence that the information source will not repudiate the supplied information.

The compliance with the above-mentioned information security principles combined with precision, quality, and usability metrics can be used to estimate the trustworthiness value of the SA and COP. Each information source, link, device, and computing system involved in providing SA and generating the COP can be assigned a trustworthiness value based on the level of security primitives incorporated in its design and operation. Security analysis can be performed on the incorporated security primitives and their resilience to adversarial attacks can be analyzed for different threat models based upon which an appropriate trustworthiness value for a given source, link, device, or computing system can be determined.

A COP obtains SA and information from a set of sources $S = \{S_1, S_2, S_3, \ldots, S_N\}$. The trustworthiness of a source $S_i$ can be given as

$$\mathcal{T}_{S_i} = f\left(C_{S_i}, I_{S_i}, \mathbb{A}_{S_i}, \mathcal{A}_{S_i}, \mathcal{N}_{S_i}, P_{S_i}, Q_{S_i}, U_{S_i}\right), \tag{1}$$

where $\mathcal{T}_{S_i}$, $C_{S_i}$, $I_{S_i}$, $\mathbb{A}_{S_i}$, $\mathcal{A}_{S_i}$, $\mathcal{N}_{S_i}$, $P_{S_i}$, $Q_{S_i}$, and $U_{S_i}$ denote the trustworthiness, confidentiality, integrity, authenticity, availability, non-reputability, precision, quality, and usability, respectively, of a source $S_i$. As discussed in Section 1, the source $S_i$ could be any of the sources providing SA including HUMINT, MASINT, IMINT, OSINT, SIGINT, and GEOINT. The function $f(\cdot)$ in Equation (1) indicates that the trustworthiness $\mathcal{T}_{S_i}$ is a function of the confidentiality, integrity, authenticity, availability, non-reputability, precision, quality, and usability of a source $S_i$. This function $f(\cdot)$ can be a simple addition or weighted addition or some other combination of the metrics of source $S_i$ for confidentiality, integrity, authenticity, availability, non-reputability, precision, quality, and usability. Delay or latency of information obtained from a source also impacts its trustworthiness. A lower usability score can be assigned to a source with large delay/latency, as SA information is often time-sensitive. We note that Equation (1) captures the situation in case a HUMINT source is compromised or

less trustworthy, where a lower integrity score can be assigned to that source. Nevertheless, the detection of a compromised and less trustworthy HUMINT source requires HUMINT, MASINT, OSINT, SIGINT and other intelligence gathering means.

To communicate the SA information from a source to the COP builder, there can be many nodes (or devices), such as relay nodes, gateway nodes, and data fusion nodes, along the way. We can denote the set of these nodes as $D = \{d_1, d_2, d_3, \ldots, d_K\}$, where $K$ denotes the total number of such nodes. Similarly, there are links that connect sources to different nodes/devices and ultimately the COP builder. We can denote the set of these links as $L = \{l_1, l_2, l_3, \ldots, l_M\}$, where $M$ denotes the total number of such links. The trustworthiness of SA information at the COP builder provided by the source $S_i$ can be determined as

$$\mathcal{T}_{COP}^{S_i} = \mathcal{T}_{S_i} \cdot \prod_{j=1}^{K} \mathcal{T}_{d_j} \prod_{m=1}^{M} \mathcal{T}_{l_m}, \tag{2}$$

where $\mathcal{T}_{d_j},\ j \in \{1, 2, 3, \ldots, K\}$ and $\mathcal{T}_{l_m},\ m \in \{1, 2, 3, \ldots, M\}$ represent the trustworthiness of nodes/devices $d_j$ and the links $l_m$, respectively, along the way from information source $S_i$ to the COP builder. The trustworthiness of a node $d_j$ can be calculated as

$$\mathcal{T}_{d_j} = f\left(C_{d_j}, I_{d_j}, \mathbb{A}_{d_j}, \mathcal{A}_{d_j}\right), \tag{3}$$

where $\mathcal{T}_{d_j}$, $C_{d_j}$, $I_{d_j}$, $\mathbb{A}_{d_j}$, and $\mathcal{A}_{d_j}$ denote the trustworthiness, confidentiality, integrity, authenticity, and availability of a node $d_j$. The function $f(\cdot)$ in Equation (3) is similar to the one in Equation (1). The trustworthiness of a link $l_m$ can be calculated as

$$\mathcal{T}_{l_m} = f(C_{l_m}, I_{l_m}, \mathcal{A}_{l_m}, Q_{l_m}), \tag{4}$$

where $\mathcal{T}_{l_m}$, $C_{l_m}$, $I_{l_m}$, $\mathcal{A}_{l_m}$, and $Q_{l_m}$ denote the trustworthiness, confidentiality, integrity, availability, and quality of a link $l_m$. The quality of a link refers to the error rate of the link. The function $f(\cdot)$ in Equation (4) is similar to that in Equation (3). In Equation (3), the trustworthiness of a node can be calculated with confidentiality, integrity, and authenticity metrics, which are classical yet fundamental components for assessing the trustworthiness of a node. The availability of nodes is also included in Equation (3) for the trustworthiness calculation because higher availability reinforces higher trustworthiness. Similarly, Equation (4) also includes confidentiality, integrity, and availability. Along with the three security metrics, Equation (4) includes the quality of links, which pertains to the error rates in the links. The higher the error rate of a link is, the lower its trustworthiness score.

The trustworthiness evaluation of COP can be performed by using a weighted system where weights are assigned to sources based on their relative importance or effect on the operation. For instance, an operation that uses aircraft will put a lot of emphasis on the air picture, not only to safeguard airspace but also to understand what is taking place in the airspace. Thus, a higher weight will be assigned to the sources of air pictures in determining the trustworthiness of a system with air operations as compared to a solely land operation that does not involve any aircraft for the operation. Showing a commander the trustworthiness value of the COP as well as the trustworthiness value of sources making up the COP provides him/her the liberty to determine whether he/she would like to trust the COP or not. A seasoned commander can set his/her preferred minimum trustworthiness value of a source and/or the overall COP. The information sources that do not meet his/her minimum criterion can be discarded from the COP without compromising the trustworthiness of the entire COP.

### *4.2. Required Trustworthiness Measure (RTM)*

To assure the trustworthiness of the COP and the SA perceived by the commander, the information sources making up the COP can have a required trustworthiness measure (RTM). If an information source's trustworthiness falls below RTM, that is, $\mathcal{T}_{s_i} <$ RTM, the

information source can be omitted from the COP to preserve the trustworthiness of the COP. Mathematically, this condition can be expressed as

$$\text{COP}_{\mathcal{T}} = \bigcup_{i=1}^{n} S_i \ \forall \ \mathcal{T}_{S_i} \geq \text{RTM}. \tag{5}$$

The equation given above (Equation (5)) means that, in a trustworthiness-aware COP, denoted as $\text{COP}_{\mathcal{T}}$, making up the $\text{COP}_{\mathcal{T}}$ are only those sources $S_i$ whose trustworthiness values are greater than or equal to RTM, that is, $\mathcal{T}_{s_i} \geq$ RTM. Since there are multiple sources reporting a particular area of interest, so even if the data from a particular source are missing due to low RTM, the commander can still always trust the COP. The RTM can also be adaptive, that is, the commander can adjust the RTM value in real-time depending on the SA needs. For example, the RTM value can be increased to ensure only highly trusted and authentic sources are displayed on the COP, or it can be lowered to show more information, with the associated risk that the additional information will have low trustworthiness. The concept of adaptive RTM is analogous to the constant false alarm rate (CFAR) used by radar operators where the CFAR can be lowered to only show definite targets from background noise, interference, and clutter, or the CFAR can be set to a higher value to identify more targets with the associated risk that some of those targets could not be real targets but noise, signals bouncing off clutter, waves at sea, etc. As the trustworthiness of information feeds changes, the commander can adjust the RTM accordingly to maintain the best possible COP and SA of the operation.

## 5. Numerical Results

In this section, we present numerical examples and results that demonstrate the quantification of the trustworthiness of the COP using our proposed model (Section 4.1). We show results for two cases: (i) COP trustworthiness for a high-trust information source that incorporates security primitives, and (ii) COP trustworthiness for a low-trust information source that does not incorporate security primitives. The trustworthiness of COP for other cases (i.e., between high-trust and low-trust information sources) can be determined following the same approach.

### *5.1. Case 1: High-Trust Information Source*

Let us consider an ISR UAV that is equipped with various sensors, such as optical sensors and infrared sensors. The UAV either sends it sensed information or the result of its on-board analytics to the ground control station (GCS) through a radio link as depicted in Figure 3. The UAV encrypts the information sent to the GCS, and also concatenates a hash of the message to help detect any intrusion. The GCS sends the encrypted information to a gateway node (GN) through a wired link. The GN is connected to a router node (RN) through a wired link, which in turn is connected to a data fusion node (DFN) through a wired link. The DFN node is connected to the COP builder node (CBN) via a wired link. We note that the number of RNs and links between the GCS and the CBN depend on the distance between the GCS and the CBN, and can vary for different settings. Nevertheless, our illustration of the COP trustworthiness quantification (Figure 3) can be adapted for different settings. In the following, we first evaluate the trustworthiness of each source and device along the route from the source to the CBN (Figure 3). Afterwards, we evaluate the trustworthiness of links from the source to the CBN, and finally we evaluate the trustworthiness of the ISR UAV information at the CBN.

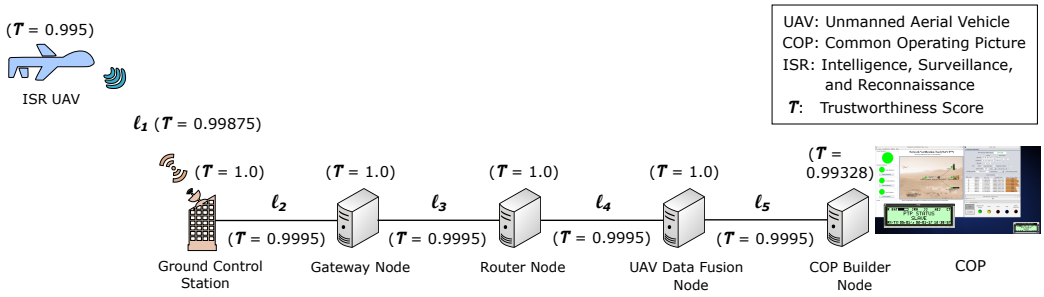


**Figure 3.** Quantification of trustworthiness of COP—case of high-trust information source.

**ISR UAV (SA Source):** We calculate the trustworthiness of the ISR UAV based on Equation (1) of our proposed model (Section 4.1). To obtain the trustworthiness of a source, we first need to obtain the score of various metrics (e.g., confidentiality, integrity, authenticity, etc.) stipulated in Equation (1) that affect the trustworthiness of the source. In the following, we calculate the score of these metrics for this case.

*Confidentiality:* For this case, the assumption is that the information gathered and analyzed by the UAV is stored in a secure memory, and is also encrypted using an advanced encryption standard (AES) or another encryption algorithm with a comparable security level. Consequently, the UAV for this case can be assigned a confidentiality score of 1. As a guideline, one can assign the highest scores (1 in this case) for security metrics, such as confidentiality, integrity, authenticity, etc., if the source employs algorithms and protocols standardized by the standardization bodies, such as the National Institute of Standards and Technology (NIST) [17].

*Integrity:* For this case, the UAV employs error correction code (ECC) memory to detect and correct $n$-bit errors in memory, and also calculates the hash-based message authentication code (HMAC) of the message or information to be transmitted to the GCS. Hence, the UAV for this case can be assigned an integrity score of 1.

*Authenticity:* For this case, the UAV can be successfully authenticated with an authentication protocol (such as the protocol in [18]), and can be assigned an authenticity score of 1.

*Availability:* For this case, the UAV is responsive to the authentication and communication protocols' messages, and is available; hence, it can be assigned an availability score of 1.

*Non-repudiability:* Since the UAV encrypts the message with its secret key, which no other source possesses, the message can be associated with the UAV. In this case, public key infrastructure (PKI) is employed by the UAV; the UAV can also sign the message with its private key, which can be verified by the CBN using the public key of the UAV, thus unambiguously binding the message to the UAV. Since the UAV in this case employs these security mechanisms that ensure that the message originated from the UAV, it can be assigned a non-repudiability score of 1.

*Precision:* In this case, the UAV is performing on-board analytics on the sensed information, the precision can be assigned based on the average precision of the AI algorithm employed for tasks, such as classification, object detection, etc. The precision score depends on the precision of a particular model or algorithm employed by the UAV. For this numerical example, we assign a precision score of 0.96. We note that different precision scores can be assigned for the source depending on the AI model.

*Quality:* The UAV obtains high-resolution images of objects of interest, and thus the quality score can be assigned as 1.

*Usability:* The UAV is mobile and can gather the information about different targets as desired; thus, the UAV can be assigned a usability score of 1.

Since, in our model, there are eight metrics that influence the trustability of the source, we assign a weight of 0.125 (i.e., $1/8 = 0.125$) to each metric. We note that different weights can be assigned to different metrics depending on the COP builder designer and the

mission needs. Using Equation (1), the trustworthiness score of the UAV $\mathcal{T}_{UAV}$ can be determined as $\mathcal{T}_{UAV} = (0.125)(1) + (0.125)(1) + (0.125)(1) + (0.125)(1) + (0.125)(1) + (0.125)(0.96) + (0.125)(1) + (0.125)(1) = 0.995$. Table 1 summarizes the scores for different metrics influencing UAV trustworthiness for this case.

**Table 1.** ISR UAV trustworthiness score.

| Metric | Score | Weightage |
|---|---|---|
| Confidentiality | 1.0 | 0.125 |
| Integrity | 1.0 | 0.125 |
| Authenticity | 1.0 | 0.125 |
| Availability | 1.0 | 0.125 |
| Non-reputability | 1.0 | 0.125 |
| Precision | 0.96 | 0.125 |
| Quality | 1.0 | 0.125 |
| Usability | 1.0 | 0.125 |
| $\mathcal{T}_{UAV}$ | 0.995 | – |

**Ground Control Station:** Here, we calculate the trustworthiness of the GCS based on Equation (3) of our proposed model (Section 4.1). To obtain the trustworthiness of a node, we first need to obtain the scores of various metrics (i.e., confidentiality, integrity, authenticity, availability, non-repudiation) stipulated in Equation (3) that affect the trustworthiness of a node. In the following, we calculate the score of these metrics for this case.
*Confidentiality:* In this case, the encrypted information from the UAV is relayed by the GCS to the GN, and thus for the GCS can be assigned a confidentiality score of 1.
*Integrity:* The GCS also relays the HMAC of the message sent by the UAV, and so an integrity score of 1 can be ascribed to GCS.
*Authenticity:* For this case, the GCS can be successfully authenticated with an authentication protocol, and thus an authenticity score of 1 can be attributed to the GCS.
*Availability:* Assuming that the GCS is responsive to the authentication and other protocols' messages, and is available, its availability score can be assigned as 1.

Since, in our model, there are four metrics that influence the trustability of the node, we assign a weight of $1/4 = 0.25$ to each metric. We note that different weights can be assigned to different metrics depending on the COP builder designer and the mission needs. Using Equation (3), the trustworthiness score of the GCS $\mathcal{T}_{GCS}$ can be determined as $\mathcal{T}_{GCS} = (0.25)(1) + (0.25)(1) + (0.25)(1) + (0.25)(1) = 1$.

**Gateway Node:** The trustworthiness of the GN can be calculated similarly to that for the GCS based on Equation (3), and can be given as $\mathcal{T}_{GN} = (0.25)(1) + (0.25)(1) + (0.25)(1) + (0.25)(1) = 1$.

**Router Node:** The trustworthiness of the RN can be calculated similarly to that for the GCS based on Equation (3), and can be given as $\mathcal{T}_{RN} = (0.25)(1) + (0.25)(1) + (0.25)(1) + (0.25)(1) = 1$.

**Data Fusion Node:** The trustworthiness of the DFN can be calculated similarly to that for the GCS based on Equation (3), and can be given as $\mathcal{T}_{DFN} = (0.25)(1) + (0.25)(1) + (0.25)(1) + (0.25)(1) = 1$.

**Link $l_1$ or $l_{UAV-GCS}$:** Here, we calculate the trustworthiness of the radio link between the ISR UAV and the GCS based on Equation (4) of our proposed model (Section 4.1). To obtain the trustworthiness of a link, we first need to obtain the score of various metrics (i.e., confidentiality, integrity, availability, and quality) stipulated in Equation (4)

that affect the trustworthiness of a link. In the following, we calculate the scores of these metrics for this case.
*Confidentiality:* Since the UAV encrypts the information to be sent, and this encrypted information traverses through the radio link between the UAV and GCS, the confidentiality score for $l_1$ or $l_{UAV-GCS}$ can be assigned as 1.
*Integrity:* Since the HMAC of the message is transmitted along with the message in this case, $l_1$ can be ascribed an integrity score of 1.
*Availability:* Assuming that the radio link can carry the messages and is not overloaded with data traffic nor is affected by any denial-of-service attack, an availability score of 1 can be attributed to $l_1$.
*Quality:* Here, the quality of a link can be referred to as its bit error rate. Assuming a bit error rate of $5 \times 10^{-3}$ [19], the quality score for $l_1$ can be calculated as 0.995 (i.e., $1 - 0.005$).

Since, in our model, there are four metrics that influence the trustability of a link, we assign a weight of 0.25 (i.e., 1/4 = 0.25) to each metric, although different weights can be assigned depending on mission needs. Using Equation (4), the trustworthiness score of the links $l_1$ or $l_{UAV-GCS}$ can be determined as $\mathcal{T}_{l_1} = (0.25)(1) + (0.25)(1) + (0.25)(1) + (0.25)(0.995) = 0.99875$.

**Link $l_2$ or $l_{GCS-GN}$:** Here, we calculate the trustworthiness of the wired link $l_2$ or $l_{GCS-GN}$ between the GCS and the GN that connects the GCS to the core network based on Equation (4). In the following, we calculate the score of the metrics that affect the trustworthiness of the link for this case.
*Confidentiality:* Since the encrypted information traverses the wired link between the GCS and the GN, $l_2$ or $l_{GCS-GN}$ can be assigned a confidentiality score of 1.
*Integrity:* Since the HMAC of the message is transmitted along with the message on the link $l_2$ in this case, the integrity score for $l_2$ can be ascribed as 1.
*Availability:* Assuming that the link can carry the messages and is not overloaded with data traffic nor is affected by any denial-of-service attack, an availability score of 1 can be attributed to $l_2$.
*Quality:* Assuming a bit error rate of $48 \times 10^{-5}$ [20], the quality score for $l_2$ can be calculated as $1 - 0.00048 = 0.99952$.

Since, in our model, there are four metrics that influence the trustability of a link, we assign a weight of 0.25 (i.e., 1/4 = 0.25) to each metric, although different weights can be assigned depending on mission needs. Using Equation (4), the trustworthiness score of the link $l_2$ or $l_{GCS-GN}$ can be determined as $\mathcal{T}_{l_2} = (0.25)(1) + (0.25)(1) + (0.25)(1) + (0.25)(0.99952) = 0.99988$.

**Link $l_3$ or $l_{GN-RN}$:** The trustworthiness of the wired link $l_3$ or $l_{GN-RN}$ between the GN and the RN in the core network can be calculated similarly to the wired link $l_2$, and can be given as $\mathcal{T}_{l_3} = (0.25)(1) + (0.25)(1) + (0.25)(1) + (0.25)(0.99952) = 0.99988$.

**Link $l_4$ or $l_{RN-DFN}$:** The trustworthiness of the wired link $l_4$ or $l_{RN-DFN}$ between the RN and the DFN can be calculated similarly to the wired link $l_2$, and can be given as $\mathcal{T}_{l_4} = (0.25)(1) + (0.25)(1) + (0.25)(1) + (0.25)(0.99952) = 0.99988$.

**Link $l_5$ or $l_{DFN-CBN}$:** The trustworthiness of the wired link $l_5$ or $l_{DFN-CBN}$ between the DFN and the CBN can be calculated similarly to the wired link $l_2$, and can be given as $\mathcal{T}_{l_5} = (0.25)(1) + (0.25)(1) + (0.25)(1) + (0.25)(0.99952) = 0.99988$.

Now that we have calculated the trustworthiness of the ISR UAV as well as all the nodes and links in the path between the UAV and the CBN, we can calculate the trustworthiness of SA information provided by the ISR UAV at the CBN using Equation (2) as:

$$\begin{aligned}\mathcal{T}_{COP}^{UAV} &= \mathcal{T}_{UAV} \cdot \mathcal{T}_{GCS} \cdot \mathcal{T}_{GN} \cdot \mathcal{T}_{RN} \cdot \mathcal{T}_{DFN} \cdot \\ &\quad \mathcal{T}_{l_1} \cdot \mathcal{T}_{l_2} \cdot \mathcal{T}_{l_3} \cdot \mathcal{T}_{l_4} \cdot \mathcal{T}_{l_5} \\ &= (0.995)(1)(1)(1)(1) \times \\ &\quad (0.99875)(0.99988)(0.99988)(0.99988)(0.99988) \\ &= 0.99328\end{aligned}$$

### 5.2. Case 2: Low-Trust Information Source

Let us consider a motion sensor (MS) that detects nearby motion (of people or objects). The MS can be a part of a wireless sensor network (WSN) and transmits its sensed information to a cluster head node (CHN) of the WSN as depicted in Figure 4. Since MS is a low-power and low-cost device, we assume that this information is transmitted in plaintext to the CHN. Further, we assume that no message hash is appended to the message. The CHN sends the plaintext information to a GN through a wired link. The gateway node is connected to RN through a wired link, which in turn is connected to a DFN through a wired link. The DFN node is connected to the CBN via a wired link (Figure 4). In the following, we first evaluate the trustworthiness of the SA information source, and each node and link along the route from the information source to the CBN, and afterwards, we evaluate the trustworthiness of MS information at the CBN.

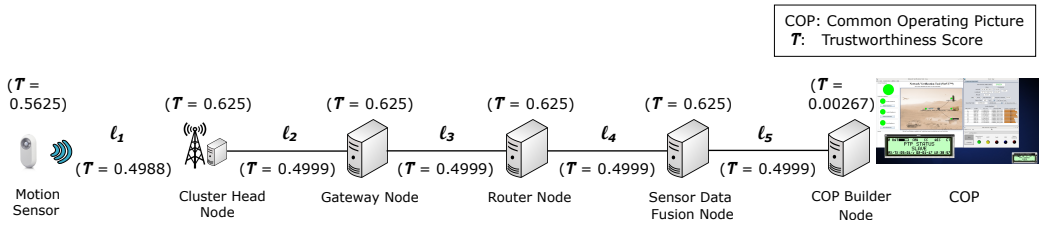


**Figure 4.** Quantification of trustworthiness of COP—case of low-trust information source.

**Motion Sensor (SA Source):** Here, we calculate the trustworthiness of the MS based on Equation (1) of our proposed model (Section 4.1). We first need to obtain the scores of various metrics stipulated in Equation (1) that affect the trustworthiness of a source. In the following, we calculate the score of these metrics for this case.

*Confidentiality:* In this case, we assume that the information gathered is not encrypted but is stored in private memory, which is not accessible to unauthorized parties. Thus, the MS for this case can be assigned a confidentiality score of 0.3. For less trustworthy sources not employing standardized protocols, the score for the security metrics can be assigned based on the overall security assessment of the source. Encryption, for example, is a primary means for ensuring confidentiality, and constitutes about 70% of the confidentiality score. For our considered example, the assumption is that the information is not encrypted, which results in a 70% penalty on the confidentiality score, while the employment of private memory and storage control permits 30% of the confidentiality score, which results in an overall confidentiality score of 0.3 for the source. We note that this weightage assignment is not standard, but just a guideline, and COP designers can choose different weightage for different aspects of the confidentiality metric.

*Integrity:* In this case, the MS employs error correction code (ECC) memory to detect and correct $n$-bit errors in memory, but does not calculate the HMAC of the message to be transmitted to the CHN. Hence, the integrity score for MS for this case can be assigned equal to 0.2.

*Authenticity:* Since the MS in this case does not incorporate security primitives, the MS cannot be authenticated with an authentication protocol (such as the protocol in [18]), and can be assigned an authenticity score of 0.

*Availability:* Since the CBN receives data from the MS periodically, an availability score of 1 can be attributed to the MS.

*Non-repudiability:* Since the MS in this case does not sign the message with its private key nor does it encrypt the messages with its secret key, it can be ascribed a non-repudiability score of 0.
*Precision:* With the assumption that the MS can detect nearby motion with 100% precision [21], we assign it a precision score of 1.
*Quality:* The MS can obtain good quality signals regarding nearby motion, and thus its quality score can be assigned as 1.
*Usability:* The motion sensors can be installed at different places, in particular places with restricted entry, to detect nearby motion; hence, a usability score of 1 can be attributed to the MS.

Since, in our model, there are eight metrics that influence the trustability of the source, we assign a weight of 0.125 (i.e., 1/8 = 0.125) to each metric, although different weights can be assigned to different metrics depending on the mission needs. Using Equation (1), the trustworthiness score of the MS $\mathcal{T}_{MS}$ can be determined as $\mathcal{T}_{MS} = (0.125)(0.3) + (0.125)(0.2) + (0.125)(0) + (0.125)(1) + (0.125)(0) + (0.125)(1) + (0.125)(1) + (0.125)(1) = 0.5625$.

**Cluster Head Node:** Here, we calculate the trustworthiness of the CHN based on Equation (3). In the following, we calculate the score of various metrics that affect the trustworthiness of a node.
*Confidentiality:* In this case, the plaintext information from the MS is relayed by the CHN to the GN. The message itself is stored in private in the CHN, and is not accessible to unauthorized parties, and thus a confidentiality score equal to 0.3 can be assigned to the CHN.
*Integrity:* The messages obtained from the MS are stored in ECC memory in the CHN, but no HMAC is calculated at the CHN, and thus an integrity score of 0.2 can be ascribed to CHN.
*Authenticity:* The CHN can be successfully authenticated (with an authentication protocol), and thus an authenticity score of 1 can be attributed to the CHN.
*Availability:* With the assumption that the CHN is responsive to the authentication messages and is available, its availability score can be assigned as 1.

Since, in our model, there are four metrics that influence the trustability of the node, we assign a weight of $1/4 = 0.25$ to each metric, although different weights can be assigned to different metrics depending on the mission needs. Using Equation (3), the trustworthiness score of the CHN $\mathcal{T}_{CHN}$ can be determined as $\mathcal{T}_{CHN} = (0.25)(0.3) + (0.25)(0.2) + (0.25)(1) + (0.25)(1) = 0.625$.

**Gateway Node:** The trustworthiness of the GN can be calculated similarly to that for the CHN based on Equation (3), and can be given as $\mathcal{T}_{GN} = (0.25)(0.3) + (0.25)(0.2) + (0.25)(1) + (0.25)(1) = 0.625$.

**Router Node:** The trustworthiness of the RN can be calculated similarly to that for the CHN based on Equation (3), and can be given as $\mathcal{T}_{RN} = (0.25)(0.3) + (0.25)(0.2) + (0.25)(1) + (0.25)(1) = 0.625$.

**Data Fusion Node:** The trustworthiness of the DFN can be calculated similarly to that for the CHN based on Equation (3), and can be given as $\mathcal{T}_{DFN} = (0.25)(0.3) + (0.25)(0.2) + (0.25)(1) + (0.25)(1) = 0.625$.

**Link $l_1$ or $l_{MS-CHN}$:** Here, we calculate the trustworthiness of the wireless link between the MS and the CHN based on Equation (4) of our proposed model (Section 4.1). In the following, we calculate the score of various metrics (i.e., confidentiality, integrity, availability, and quality) stipulated in Equation (4) that affect the trustworthiness of a link.
*Confidentiality:* Since the MS sends the information in plaintext (i.e., without encryption) to the CHN over the wireless link, the confidentiality score for $l_1$ or $l_{MS-CHN}$ can be assigned as 0.

*Integrity:* Since no hash (or HMAC) of the message is transmitted from the MS and the CHN in this case, the integrity score for $l_1$ can be ascribed as 0.
*Availability:* Assuming that the wireless link between the MS and the CHN can carry the messages and is not overloaded with data traffic nor is affected by any denial-of-service attack, an availability score of 1 can be attributed to $l_1$.
*Quality:* Here, the quality of a link can be referred to as its bit error rate. Assuming a bit error rate of $5 \times 10^{-3}$ [19], the quality score for $l_1$ can be calculated as $1 - 0.005 = 0.995$.

Since, in our model, there are four metrics that influence the trustability of a link, we assign a weight of 0.25 (i.e., 1/4 = 0.25) to each metric, although different weights can be assigned depending on mission needs. Using Equation (4), the trustworthiness score of the link $l_1$ or $l_{MS-CHN}$ can be determined as $\mathcal{T}_{l_1} = (0.25)(0) + (0.25)(0) + (0.25)(1) + (0.25)(0.995) = 0.49875$.

**Link $l_2$ or $l_{CHN-GN}$:** Here, we calculate the trustworthiness of the wired link $l_2$ or $l_{CHN-GN}$ between the CHN and the GN that connects the CHN to the core network based on Equation (4). In the following, we calculate the score of the metrics that affect the trustworthiness of the link for this case.
*Confidentiality:* Since the plaintext information (without encryption) sent from the MS traverses the wired link between the CHN and the GN, the confidentiality score for $l_2$ or $l_{CHN-GN}$ can be assigned as 0.
*Integrity:* Since no HMAC of the message is transmitted along with the message on the link $l_2$ in this case, the integrity score for $l_2$ can be ascribed as 0.
*Availability:* Assuming that the link can carry the messages and is not overloaded with data traffic nor is affected by any denial-of-service attack, an availability score of 1 can be attributed to $l_2$.
*Quality:* Assuming a bit error rate of $48 \times 10^{-5}$ [20], the quality score for $l_2$ can be calculated as $1 - 0.00048 = 0.99952$.

Since, in our model, there are four metrics that influence the trustability of a link, we assign a weight of 0.25 (i.e., 1/4 = 0.25) to each metric. Using Equation (4), the trustworthiness score of the link $l_2$ or $l_{GCS-GN}$ can be determined as $\mathcal{T}_{l_2} = (0.25)(0) + (0.25)(0) + (0.25)(1) + (0.25)(0.99952) = 0.49988$.

**Link $l_3$ or $l_{GN-RN}$:** The trustworthiness of the wired link $l_3$ or $l_{GN-RN}$ between the GN and the RN in the core network can be calculated similarly to the wired link $l_2$, and can be given as $\mathcal{T}_{l_3} = (0.25)(0) + (0.25)(0) + (0.25)(1) + (0.25)(0.99952) = 0.49988$.

**Link $l_4$ or $l_{RN-DFN}$:** The trustworthiness of the wired link $l_4$ or $l_{RN-DFN}$ between the RN and the DFN can be calculated similar to the wired link $l_2$, and can be given as $\mathcal{T}_{l_4} = (0.25)(0) + (0.25)(0) + (0.25)(1) + (0.25)(0.99952) = 0.49988$.

**Link $l_5$ or $l_{DFN-CBN}$:** The trustworthiness of the wired link $l_5$ or $l_{DFN-CBN}$ between the DFN and the CBN can be calculated similarly to the wired link $l_2$, and can be given as $\mathcal{T}_{l_5} = (0.25)(0) + (0.25)(0) + (0.25)(1) + (0.25)(0.99952) = 0.49988$.

Now that we have calculated the trustworthiness of the MS as well as all the nodes and links in the path between the MS and the CBN for this case, we can calculate the trustworthiness of SA information provided by the MS at the CBN using Equation (2) as:

$$\begin{aligned}
\mathcal{T}_{COP}^{MS} &= \mathcal{T}_{MS} \cdot \mathcal{T}_{CHN} \cdot \mathcal{T}_{GN} \cdot \mathcal{T}_{RN} \cdot \mathcal{T}_{DFN} \cdot \\
&\quad \mathcal{T}_{l_1} \cdot \mathcal{T}_{l_2} \cdot \mathcal{T}_{l_3} \cdot \mathcal{T}_{l_4} \cdot \mathcal{T}_{l_5} \\
&= (0.5625)(0.625)(0.625)(0.625)(0.625) \times \\
&\quad (0.49875)(0.49988)(0.49988)(0.49988)(0.49988) \\
&= 0.00267
\end{aligned}$$

We clarify that this example can have different cases; for example, the CHN node could encrypt the information and could also calculate the message hash before sending it

to the GN, and thus would result in a different trustworthiness score of the MS at the CBN. However, we present this case to illustrate how a trustworthiness score from an SA source appears at the CBN node. The trustworthiness score at the CBN node depends not only on the security capabilities of the SA information source but also on the devices and links along the path from the SA information source to the CBN.

## 6. Conclusions and Future Research Directions

Situational awareness (SA) is crucial for successful operations in many application domains, such as humanitarian missions, surveillance, search and rescue missions, and national security. This paper provides an overview of SA from an air force perspective. This paper further contemplates security and trust issues in SA and the potential effect of these issues on the perceived SA and decision-making of commanders and operators. This paper also proposes a simple yet powerful model for quantifying the trustworthiness of an SA system. This paper then presents numerical examples that demonstrate the quantification of the trustworthiness of an SA system using our proposed model. The numerical results show that a high-trust information source that incorporates security primitives attains a trustworthiness score of 0.9933 or 99.33%, whereas a low-trust information source achieves a trustworthiness score of merely 0.00267 or 0.267% at the common operating picture. The trustworthiness of other sources with intermediate trust levels can be calculated similarly using our proposed model. These trustworthiness scores at the common operating picture provide guidance to the commander on how much trust he/she can put in the information received by a particular information source. This paper is the first of its kind to develop a model for assessing the trustworthiness of SA systems and can help stimulate further research in this area.

Accurate quantification of the trustworthiness of SA systems needs further research. Automated tools need to be developed that can assist the commanders in determining the trustworthiness of different sources in the common operating picture. Furthermore, since the trustworthiness of SA sources and devices is crucial to gain the trust of a commander in the common operating picture, different security approaches can be incorporated in the design of SA sources and equipment to provide resilience against adversarial attacks. Finally, tradeoffs exist in balancing security with constraints on the performance, area, and cost of SA devices and systems.

One interesting avenue of future research is to further attest our proposed model using human factor experiments [22]. The detailed human-subject experiments can be used to validate the effectiveness of the proposed model in enhancing situational awareness. Such a study can be used to experimentally demonstrate that showing the trustworthiness information of all the sources in the common operating picture help enhance the situational awareness of the commander.

**Author Contributions:** Conceptualization, A.M.; methodology, A.M.; software, A.M.; validation, A.M.; formal analysis, A.M.; investigation, A.M. and A.A.; resources, A.M.; data curation, A.M.; writing—original draft preparation, A.M.; writing—review and editing, A.M., A.A., K.P. and J.K.; visualization, A.M.; supervision, A.M.; project administration, A.M. and A.A.; funding acquisition, A.M. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was supported in part by the Air Force Research Laboratory (AFRL) Information Directorate (RI), through the Air Force Office of Scientific Research (AFOSR) Summer Faculty Fellowship Program®, Contract Numbers FA8750-15-3-6003, FA9550-15-0001 and FA9550-20-F-0005.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

**Acknowledgments:** The authors would like to acknowledge Erik Blasch for his support and guidance on this research as well as for providing his valuable feedback and revision of this manuscript.

**Conflicts of Interest:** The authors declare no conflicts of interest.

**Disclaimer:** To the best of the authors' knowledge, the presented research in this manuscript falls under the category of fundamental/basic research and poses no public harm. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the AFRL and AFOSR.

**Abbreviations**

The following abbreviations are used in this manuscript:

| | |
|---|---|
| SA | Situational awareness |
| DOD | Department of Defense |
| OODA | observe–orient–decide–act |
| USAF | United States Air Force |
| CC | Command and control |
| UAV | Unmanned aerial vehicles |
| ISR | Intelligence, surveillance, and reconnaissance |
| HUD | Heads-up display |
| HMD | Helmet-mounted display |
| HUMINT | Human intelligence |
| MASINT | Measurement and signature intelligence |
| IMINT | Imagery intelligence |
| OSINT | Open source intelligence |
| SIGNIT | Signals intelligence |
| GEOINT | Geospatial intelligence |
| COP | Common operating picture |
| UDOP | User-defined operating picture |
| AI | Artificial intelligence |
| ICT | Information and communications technology |
| RTM | Required trustworthiness measure |
| CFAR | Constant false alarm rate |
| GCS | Ground control station |
| GN | Gateway node |
| RN | Router node |
| DFN | Data fusion node |
| CBN | COP builder node |
| AES | Advanced encryption standard |
| ECC | Error correction code |
| HMAC | Hash-based message authentication code |
| PKI | Public key infrastructure |
| MS | Motion sensor |
| WSN | Wireless sensor network |
| CHN | Cluster head node |
| ECC | Error correction code |

## References

1. Munir, A.; Aved, A.; Blasch, E. Situational Awareness: Techniques, Challenges, and Prospects. *AI* **2022**, *3*, 55–77. [CrossRef]
2. Spick, M. *The Ace Factor: Air Combat and the Role of Situational Awareness*; Naval Institute Press: Annapolis, MD, USA, 1988.
3. Munir, A.; Blasch, E.; Aved, A.; Ratazzi, E.P.; Kong, J. Security Issues in Situational Awareness: Adversarial Threats and Mitigation Techniques. *IEEE Secur. Priv.* **2022**, *20*, 51–60. [CrossRef]
4. McKay, B.; McKay, K. The Tao of Boyd: How to Master the OODA Loop. 2019. Available online: https://www.artofmanliness.com/articles/ooda-loop/ (accessed on 14 August 2019).

5. Endsley, M.R. Toward a Theory of Situation Awareness in Dynamic Systems. *Hum. Factors J. Hum. Factors Ergon. Soc.* **1995**, *37*, 32–64. [CrossRef]
6. Endsley, M.R. Situation Awareness Global Assessment Technique (SAGAT). In Proceedings of the IEEE National Aerospace and Electronics Conference, Dayton, OH, USA, 23–27 May 1988.
7. Nguyen, T.; Lim, C.P.; Nguyen, N.D.; Gordon-Brown, L.; Nahavandi, S. A Review of Situation Awareness Assessment Approaches in Aviation Environments. *IEEE Syst. J.* **2019**, *13*, 3590–3603. [CrossRef]
8. Hart, S.G.; Staveland, L.E. Development of NASA-TLX (Task Load Index): Results of Empirical and Theoretical Research. *Adv. Psychol.* **1988**, *52*, 139–183.
9. Taylor, R. Situational Awareness Rating Technique (SART): The Development of a Tool for Aircrew Systems Design. In Proceedings of the AGARD AMP Symposium on Situational Awareness in Aerospace Operations (AGARD-CP-478), Copenhagen, Denmark, 2–6 October 1989.
10. O'Hare, D.; Wiggins, M.; Williams, A.; Wong, W. Cognitive Task Analyses for Decision Centred Design and Training. *Ergonomics* **1998**, *41*, 1698–1718. [CrossRef] [PubMed]
11. Blasch, E.P.; Salerno, J.J.; Tadda, G.P. Measuring the Worthiness of Situation Assessment. In *High-Level Information Fusion Management and Systems Design*; Blasch, E., Bossé, E., Lambert, D.A., Eds.; Artech House: Norwood, MA, USA, 2012; pp. 315–329.
12. Endsley, M.R. The Divergence of Objective and Subjective Situation Awareness: A Meta-Analysis. *J. Cogn. Eng. Decis. Mak.* **2020**, *14*, 34–53. [CrossRef]
13. Zhang, T.; Yang, J.; Liang, N.; Pitts, B.J.; Prakah-Asante, K.O.; Curry, R.; Duerstock, B.S.; Wachs, J.P.; Yu, D. Physiological Measurements of Situation Awareness: A Systematic Review. *Hum. Factors* **2020**, *65*, 737–758. [CrossRef]
14. Robertson, J. Integrity of a Common Operating Picture in Military Situational Awareness. In Proceedings of the Information Security for South Africa (ISSA), Johannesburg, South Africa, 13–14 August 2014.
15. Roberts, P. Researchers Warn of Physics-Based Attacks on Sensors. 2018. Available online: https://securityledger.com/2018/01/researchers-warn-physics-based-attacks-sensors/ (accessed on 23 June 2020).
16. Paar, C.; Pelzl, J. *Understanding Cryptography*; Springer: Berlin/Heidelberg, Germany, 2010.
17. NIST. National Institute of Standards and Technology. 2024. Available online: https://www.nist.gov/ (accessed on 9 February 2024).
18. Giri, N.K.; Munir, A.; Kong, J. An Integrated Safe and Secure Approach for Authentication and Secret Key Establishment in Automotive Cyber-Physical Systems. In Proceedings of the Computing Conference, Virtual, 16–17 July 2020.
19. Li, B.; Jiang, Y.; Sun, J.; Cai, L.; Wen, C.Y. Development and Testing of a Two-UAV Communication Relay System. *Sensors* **2016**, *16*, 1696. [CrossRef] [PubMed]
20. Okpeki, U.; Egwaile, J.; Edeko, F. Performance and Comparative Analysis of Wired and Wireless Communication Systems using Local Area Network Based on IEEE 802.3 And IEEE 802.11. *J. Appl. Sci. Environ. Manag.* **2018**, *22*, 1727–1731. [CrossRef]
21. Liu, H.; Wang, Y.; Wang, K.; Lin, H. Turning a Pyroelectric Infrared Motion Sensor into a High-Accuracy Presence Detector by Using a Narrow Semi-Transparent Chopper. *Appl. Phys. Lett.* **2017**, *111*, 243901. [CrossRef]
22. Lee, J.D.; See, K.A. Trust in Automation: Designing for Appropriate Reliance. *Hum. Factors* **2004**, *46*, 50–80. [CrossRef] [PubMed]