Impact of Security Properties on the Quality of Information in Tactical Military Networks

Greg Cirincione
U.S. Army Research Lab
cirincione@arl.army.mil

Srikanth Krishnamurthy
University of California, Riverside
krish@cs.ucr.edu

Thomas F. La Porta
Penn State University
tlp@cse.psu.edu

Ramesh Govindan
University of Southern California
ramesh@usc.edu

Prasant Mohapatra
University of California, Davis
prasant@cs.ucdavis.edu

Abstract— **The goal of a tactical military network is to provide information superiority over an opposing force. This information superiority increases mission tempo if the information can be used to make correct decisions within time constraints. To achieve this goal, a sufficient amount of information must be received with a required quality. The information quality implicitly accounts for the level of security provided. In this paper we examine the dependencies between security and other factors that affect the information quality. We incorporate the notion of the amount of information of sufficient quality received over time as the operational information content capacity. We discuss the complex tradeoffs that arise while providing security properties: the decision maker may require certain security properties to use information, but the provision of such properties may degrade the ability of the network to deliver the required amount of information in time, thus lowering the operational information content capacity of the network.**

Keywords-securoty, qualuty of information, capacity, provenance, credibility

I. Introduction

Tactical military networks are used to gather information based upon which decisions are made. The faster, and more correctly decisions are made, the more responsive a force becomes, increasing mission tempo and allowing information superiority to be fully leveraged. Information upon which decisions are based is judged in terms of its quality in several dimensions.

Security properties have a significant impact on the amount and quality of information (QoI) conveyed over a tactical network. Just as the latency or loss experienced by a packet influences its usefulness or quality to an application, so do the security properties of the information. The QoI is impacted by security characteristics of the information source, the network that transports it, and the processes that act upon it. In this paper, our aim is to characterize the impact of security on the quality of information and in turn on the operational information content capacity.

We define a set of basic security properties that are relevant to tactical networks. Specifically we focus on information provenance, which relates to authentication of information sources and nodes that assist in transferring and processing the information, and information confidentiality. Information provenance, in turn, helps determine the credibility (or believability) of information.

We discuss the trade-offs, in terms of QoI, of security mechanisms and their impact on the ability of a network to deliver the information to a destination. For some applications it may be necessary to reduce security requirements in order to enable required information to be received. In some cases there may be out-of-band techniques to authenticate data through corroboration with independent sources, thus lowering security requirements on a particular information flow. These trade-offs must be evaluated when configuring a network. The availability of various options for trade-offs will also impact the QoI.

The remainder of the paper is organized as follows. In Section II we define QoI and operational information content capacity (OICC) which is a metric that combines the impact of QoI and capacity. In Section III we define the security properties of interest. In Section IV we discuss how the function of providing security properties interacts with the ability of the network in delivering information; this creates interesting tradeoffs in terms of the QoI. Our conclusions form Section V.

II. Quality of Information and Information Content Capacity

QoI is a composite, multi-dimensional, metric that captures the trade-offs between several components to characterize the information ultimately delivered to the application. QoI has been applied in different ways in the context of military networks [1][2], often when characterizing data generated from a sensor network [3][4]. Tactical applications may specify a desired QoI, and the network seeks to deliver this QoI efficiently. Delivery of the required QoI may be achieved through efficient resource management, adaptive protocols, or by using various modalities of information transfer.

QoI can be represented in a compact form as

$$QoI = f(I, D, P, S)$$

where *I* captures the attributes of the information source, *D* captures the characteristics of the network delivery, *P* represents the transformations of data by in-network processing, for example fusion or compression, and *S* accounts for the security properties of the system.

Several attributes of QoI are clearly specified in DoD documentation as the basis for evaluating information [1][2], but prior work has not considered any systematic way of quantifying the impact of security on QoI, or analyzing any trade-offs between those two critical aspects of military applications.

Closely related to QoI is the *operational information content capacity* (OICC) of a network. OICC quantifies the useful information (as opposed to volume of data) that can be retrieved from an operational network. The transformation of QoI into OICC includes a time dimension and must quantify the amount *and* quality of information that can be transferred across a network in the presence of multiple information flows and end nodes. In essence, OICC is related to "how many correct decisions are enabled by the information obtained from the network per unit time."

Security properties then have a two-fold influence on OICC: first, their presence or absence impacts QoI; second, providing a security property may, because it uses network resources, impact the ability of the network to deliver data, thus impacting capacity. In this paper, we focus on enumerating several security properties and discussing how these properties can impact QoI, often in subtle and complex ways.

III. Security Properties

In this section we discuss some important security properties for tactical networks. We then show how these enable decision making.

A. *Security Properties*

The first step towards understanding the impact of security on QoI requires us to model a set of fundamental security primitives or properties. We discuss (a) confidentiality, (b) provenance (including properties of authenticity and non-repudiation), (c) availability, and (d) intrusion resilience to achieve integrity. The four properties are critical in a tactical setting.

1) *Data Confidentiality*

In a tactical network, it is of paramount importance to ensure that information is available to those who are authorized to receive/decode it, and is protected from those who are not. The latter may be external (malicious) entities, compromised nodes, or simply nodes that have a lower security clearance as compared to the authorized nodes. Data confidentiality is the ability to prevent data from being leaked to unauthorized nodes.

2) *Provenance*

Data provenance provides certainty about the chain of custody of the information. This includes the origin of and operations on data from its source through its transfer to a destination. Provenance subsumes the properties of authenticity and non-repudiation. Authenticity allows peer nodes to have proof of who they are communicating with, or to validate the source of data. Non-repudiation provides proof of identity or origin to a third party; thus, for example, a communicating party cannot later deny transmitting a message or performing an operation.

Provenance may also require some type of attestation as to what operations have been performed on any information, for example, information extraction, compression or fusion. This may include some formal proof of what version of software implements a particular algorithm that operates on data [5], and a full description of the provenance of all information that has been fused.

3) *Availability*

A node or service is available if it is reachable via a given network and able to provide its critical functions. While availability is impacted by normal network failures, here we focus on the impact of security properties and attacks on availability. For example, if two nodes require a shared key to communicate, and the key expires, a server to assist with re-keying and re-authentication may be required. If this service is not available, then the ability of the nodes to communicate is lost.

An important differentiation between military tactical networks and commercial networks is that availability is often mission-critical and soldier's lives depend on the availability of the network for their survival. In a commercial network productivity or profit may be impacted but it is not life or death.

4) *Intrusion resilience*

Intrusion resilience measures how well a system withstands attacks, especially intrusion and partial compromise. Of particular interest are attacks that impact the integrity of data and/or programs. This resiliency may be provided by detecting and stopping intruders, by designing networks to be robust against attacks, or by providing the ability for the system to operate through and recover from attacks. We are concerned with the property of resiliency regardless of the mechanism used to provide it.

B. *Decision Making: Information Credibility*

Another important factor that impacts QoI is *credibility*, defined as the objective believability of information [6]. Decision-makers may vary the importance they place to the believability of information while assessing its value in the process of decision-making. The credibility of information generated by a network depends upon many factors, including the reputation of the source, the capacity or expertise of the source, and the situation under which it was generated.

The maintenance of credibility of information as it passes through a network is a function of the security properties in the network. Below we provide an overview of how several security properties impact credibility. Please refer to Figure 1 for this discussion.

1) *Data Confidentiality*

Data confidentiality may impact the situation under which information is generated. If someone generating information is ensured that no adversaries can overhear it, or understand it, they are more likely to report truthful, accurate information. If an information source believes it is being overheard, it may hide or misreport information. Therefore, the presence of a confidentiality guarantee will tend to increase credibility.

2) *Provenance*

Data provenance essentially records the chain of custody for data. It allows the recipient to understand how the information was generated, and which nodes, processes and people touched it before it was received. A full provenance report allows the information recipient to make an informed judgment of how credible information is. The presence of a provenance guarantee increases the credibility of information. This applies to authentication of a source and any processing performed on the information. Often, the ability to accurately judge credibility is as important as the amount of credibility itself.

3) *Availability*

Availability has a first and second order effect on creditability. First, if network connectivity is not available to certain nodes, or if information sources themselves are unavailable, less information may be retrieved over the network. The lack of information can directly reduce to overall credibility of a collection of information. Often multiple sources of information are important for corroboration of information.

Second, if certain security services are unavailable, because for example a server has crashed or been compromised, information credibility may drop.

4) *Intrusion resilience*

Intrusion resilience also has a second order effect on credibility. A network or service that is robust against attacks, or that can accurately detect attacks and assess their impact, will produce information whose quality is accurately evaluated. This leads to higher credibility in the information.

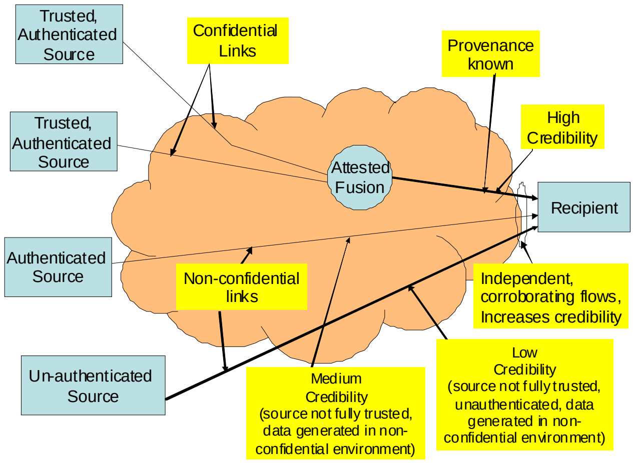
Trusted, Authenticated Source
Confidential Links
Provenance known
Trusted, Authenticated Source
High Credibility
Attested Fusion
Recipient
Authenticated Source
Non-confidential links
Independent, corroborating flows, Increases credibility
Un-authenticated Source
Medium Credibility (source not fully trusted, data generated in non-confidential environment)
Low Credibility (source not fully trusted, unauthenticated, data generated in non-confidential environment)

Figure 1. Example of Security Properties and Credibility

IV. Impact of Security Properties on QoI

In this section we discuss the impact of security properties and some mechanisms for providing them, on QoI.

A. *Data Confidentiality*

As mentioned, confidentiality is required to protect transmitted information from eavesdropping on the network and from an attacker who has compromised a node. The keys themselves are at risk of compromise and must be subject to the same confidentiality requirements as the user information.

Providing confidentiality with the use of encryption will increase security but requires processing and thus will affect the quality of information delivered through its impact on the characteristics of network delivery. As an example, ensuring the confidentiality of large volumes of video data could be difficult and in some cases even infeasible depending on the security infrastructure available. However, if the same *information* may be delivered as text data (but with lower fidelity) it is significantly easier to provide a high degree of associated confidentiality.

Varying strengths of confidentiality may lead to varying impacts on the QoI. Encryption may either be performed using secret keys or using a public key system, which requires a Public Key Infrastructure (PKI), each of which presents its own trade-offs in terms of QoI.

With secret keys, the processing overhead incurred for encryption is relatively low [7]. However, these secret keys will have to be distributed. Key distribution by itself is a challenge. For example, if a network allows nodes to cache and serve data to each other [8], or perform processing functions like information fusion, then data must be routed through these nodes to take advantage of the service. The higher the number of such nodes that are supported in the network, the better the performance improvement will be. Each of these nodes will need to share keys so that information transfer will be confidential.

Providing nodes with large sub-sets of the available keys would improve performance (shorter routes); however, such a system be more susceptible to eavesdropping and thus, would lead to lower degrees of confidentiality.

In Figure 2 we show the average path length vs. number of neighbors through which a node may route packets for a network of 200 nodes in which source and destination pairs are randomly chosen. It is evident that as the number of neighbors that route packets increases, perhaps because they share keys, the path length is reduced which will improve the performance of individual flows as well as increase the capacity of a network.. Conversely, if there are fewer routing options (i.e., few nodes which may route packets), path length increases.

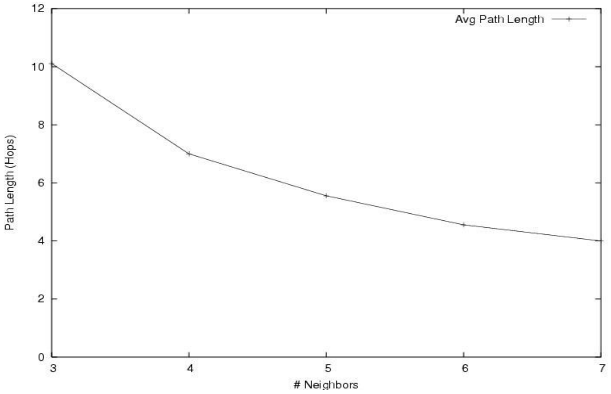

Figure 2. Impact of number of next-hop nodes on path length.

The key distribution function itself will consume overhead and this will impact the achievable performance. In general, key distribution and management approaches have an impact on security as well as the performance of the network and its information content. Thus, there is an inherent trade-off between the data delivery capabilities (performance) and security in this context.

Public key encryption techniques provide stronger security (more difficult to break the encryption), but present challenges in terms of certifying keys and adding computational complexity [7]. Public keys have to be certified by authorities (similar to authentication with provenance). Certification, as authentication, comes with a price – overhead. In a tactical setting, one can envision the certification authority to be a commander or a group leader. Depending on the classification of the data (the level of authentication desired) one may envision a hierarchy of authorities. The certificate authorities may be mobile and finding them and dynamically obtaining certification will consume overhead. In some cases, there may be no connectivity to an authority. One can choose to bypass certification to improve performance; however, this comes at the risk of man-in-the-middle attacks by compromised adversaries and thus, would weaken the security in the delivered QoI.

One option is the pre-provision certificates for public keys in nodes as they are deployed for a mission. This approach may limit flexibility as missions progress and information requirements change.

B. Provenance

Data provenance quantifies the chain of custody of information, including the origin of, and operations on data from its source through its transfer to a destination. Provenance subsumes the properties of authenticity and non-repudiation. Authenticity allows peer nodes to have proof of who they are communicating with, or to validate the source of data. Non-repudiation provides proof of identity or origin to a third party such that a communicating party cannot later deny transmitting a message or performing an operation.

To determine provenance, the first step is to ensure that the properties of authenticity and non-repudiation apply to the source node. If the source node cannot be authenticated, there is no provenance associated with the generated data. Likewise, without a non-repudiation property, a third party cannot verify the source of the information. The non-repudiation property should apply to the transit nodes as well, i.e., the nodes that forward the data from the source to its destination.

Because provenance is related to the “chain of evidence,” if a transit node operates on the data, exactly what operation was performed must be certifiable. The interaction between provenance and the achievable performance in the network is complex and not well understood.

While providing provenance one should ensure that

- An adversary (or a group of adversaries) cannot modify the information chain (source to destination though a trusted members) by adding fake entries, or removing entries from valid users.
- People who forward the information cannot repudiate their activities impacting the information.
- Decision makers can verify authenticity of an information chain without the requirement to learn more details, such as the content of the information.

Decision makers should be able to detect the following:

- Forgery of individual provenance records
- The sequence of records in the chain.
- How nodes were compromised, so as to determine if other nodes are threatened.

Most existing research focused on provenance relies on recording the entire history of information, annotations, information-flow recoding etc. However, in a heterogeneous dynamic network, the provision of provenance and its impact on the information quality and content is not well understood. Moreover, the history-based approaches could impose various resource constraints in terms of bandwidth and storage. The risk of explosion and the complexities related to the history-based approaches further limits their applicability.

Typically providing provenance can be done in the following generic ways. Strong provenance is provided by requiring the operator node to include some form of information that uniquely attests that it performed the operation. Digital signatures or the use of private keys to encrypt the information are mechanisms that can support strong provenance. Strong provenance provides a means for ensuring non-repudiation i.e., a node that includes this unique information is responsible for the operations on the message and its contents up to the point where the “node signs the message in some form.” However, signing messages incurs significant processing overhead. Resource-limited nodes may not be able digitally sign messages. Signing heavy volumes of data could degrade the performance to unacceptable levels.

Finally, a weak form of provenance can be obtained by witnesses that observe actions. The degree of provenance associated with an operation observed by a witness is directly dependent on the trustworthiness of the witness. Moreover, if one has to ensure provenance, data will have to be routed via dense areas and this could increase congestion and thus, the achievable performance. In summary, all of these high level strategies have direct implications on the QoI achievable in the network, which includes how QoI is impacted by the overhead of security mechanisms.

We summarize three important aspects of provenance below.

1) Operator provenance

A node can be required to include information that uniquely ties it to the operation that it performs. As described earlier, using digital signatures or simply private keys to encrypt the message are mechanisms that can help satisfy this requirement. The questions that arise are: (a) How effective is a signature in uniquely tying the operation to the node performing the operation? Stated otherwise, how likely is it that an adversarial node can override this security property to destroy the provenance? and, (b) How does the provision of operator provenance affect the data delivery performance and the QoI?

To illustrate these issues, consider that digital signatures serve as the mechanisms for supporting operator provenance. A stronger signature would ensure higher provenance but will impact data delivery in terms of throughput and delay. A weaker signature can be more easily reproduced by an adversary, but will have a lower impact on data delivery performance.

Different applications will have different requirements in terms of the provenance and performance. Further, in a heterogeneous network, different nodes will have different capabilities in terms of providing operator provenance. From the perspective of mechanisms, different processing capabilities and, thus, will not be able to either sign or verify signatures. Together these will have an impact on the QoI metric.

2) Authentication

Operator provenance is unlikely to be of use in cases where a node may be compromised; its signatures have been stolen, or is of unknown identity. Here, a higher level known entity (such as a decision maker – or a digital counterpart) will have to authenticate a node. The impact of authentication is very much dependent on the location of the higher level authenticating entity. If this node is further away (a decision maker overseeing a large group of soldiers) or the channel qualities are poor, obtaining the authentication may be time-consuming and in some extreme cases, may be impossible. There is then, an inherent trade-off between information quality, provenance and performance. If obtaining the authentication takes time, the data may become somewhat stale. The question then would be whether there is a sufficient level of QoI for the application. If this is not the case, the question would be whether a weaker provenance is sufficient – but accepting the potential QoI degradation?

3) Witnesses

A node may simply depend on other observing nodes (witnesses) to provide provenance on a node's actions. This depends on the number of observers, and the trust that the node seeking provenance, has on these observers. Clearly, this depends on the density of the network, mobility and the likelihood of having colluding adversaries, which may be mitigated by artificial diversity among the nodes. The use of interference mitigation techniques (such as directional antennas or MIMO) may affect the ability of nodes to witness transactions. These factors will result in an associated uncertainty with regards to the provenance that can be provided but will reduce the overhead incurred or mitigate interference and thus, could result in better data delivery capabilities.

Modeling secured provenance is extremely complex in the case of multihop transmission of information among the heterogeneous networks. It will be even more complex if we assume the network is highly mobile, which is the normal mode of operation in tactical environments.

V. Relationship between Security, Data Delivery, and QoI: OICC

As is evident from the discussions in the previous Section, information capacity and security are fundamentally inter-related. The trade-offs between security, data delivery and QoI are not well understood. We emphasize the importance and complexity of this trade-off. The results characterizing these trade-offs are critical to determining the best QoI that a network may achieve.

Intuitively, one can argue that securing information based on any of the properties discussed above results in an overhead either in terms of additional information to be shared between the network entities, higher delays incurred in ensuring security, or administrative overhead to address attacks or false alerts. One can further argue that this in turn leads to a discount in what information can be carried over the network. For example, information theory clearly indicates that data confidentiality (secrecy) from an eavesdropper is possible at the expense of transmission rate [9].

Similarly the bandwidth and processing resources required to authenticate parties contributes to security overhead. Certain choices made in order to enable secure transmissions, e.g., establishing/distributing keys, leads to resource consumption that would otherwise have been used for data transmission.

We argue that the relationship between the fundamental performance metric in a tactical network, the operational information content capacity, and information security is far more complex than simply quantifying security overhead. This is precisely due to the fact that the metric is based on the quality of information (QoI). Very simply put, in many applications, various security properties may be required to ensure a high (or acceptable) QoI; in other words, without these security properties in place, one cannot achieve high operational capacity. Thus, the operational capacity may be very low even when a high throughput in bits/sec/Hz is achieved because the information cannot be relied upon.

Consider the following example. A mission is launched to locate a specific person who is suspected to be in a certain area. Models predict that a network can either provide a high quality video stream from cameras in that area, without authentication. This is a direct consequence of the available network resources and security services available to certain sources i.e., the portion of the network capable of carrying video is not secured and the camera lacks the credentials to be authorized. Alternatively, an informant is in the area carrying an authenticated device capable of sending text messages over a secured channel, i.e., an authenticated, confidential channel.

Depending on the application, the user will then make a decision on whether he/she would like the video, the text message, or if either is equally acceptable.

For example, if the recipient of the video stream will run sophisticated gait analysis and facial recognition software, perhaps a large field of view and the ability to process stored video long after it has been received will make the video stream desirable even without the security properties. Of course, for full provenance, the software executing the analysis and recognition requires attestation. Alternatively, if action is to be taken immediately upon receiving positive identification of the person of interested, then there might not be time to execute the analysis software and a direct authenticated identification from a trusted source would be better.

If multiple sources of information are considered the trade-offs become more complex. For example, the video source and text source could be used to corroborate each other, thus improving the credibility of the information if the two sources are independent. In addition, it may be possible to compress the video in this case, thus lowering its bit rate at the cost of degrading the video quality, if the text message corroboration can re-gain to QoI lost because of the video compression.

This example illustrates several dimensions of the security trade-offs for QoI. The most intuitive security-QoI tradeoff is simple: often, increased security results in lower performance for data delivery for both the information flow of interest and other ongoing flows in the network. However, the QoI increase due to the security property may outweigh the loss in capacity. There is also a counterintuitive trade-off: sometimes it is easier to secure a lower volume piece of information than a high volume piece of information, thus making the lower rate information have higher QoI than the high rate information. This type of data reduction will increase the operational information content capacity of the network thus potentially improving the QoI of other missions.

VI. Conclusion

In this paper we discussed the impact of security properties in a tactical network on the QoI and OICC delivered to applications. We reviewed several key security properties and mapped them into QoI and credibility, an important factor used when assessing if decisions may be based on received information. Finally, we described the impact of security properties on OICC; these include a composite impact on the QoI of the information and the capacity of the network.

Acknowledgment

Research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-09-2-0053. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on.

References

[1] Department of Defense. “Joint Publication 6-0: Joint Communications System,” 20 March 2006.

[2] Headquarters, Department of the Army. “Field Manual 6-0: Mission Command: Command and Control of Army Forces,” August 2003.

[3] Bisdikian, C., Verma, D., Kaplan, L., Srivastava, M., Thornley, D. “Defining Quality of Information and Metadata for Sensor-originating information,” *4th USMA Network Science Workshop*, West Point, NY, October 28-30, 2009.

[4] Bisdikian, C., Kaplan, L., Srivastava, M., Thornley, D, Verma, D., Young, R. “Building Principles for a Quality of Information Specification for Sensor Information,” *12th International Conference on Information Fusion*, Seattle, WA, July 6-9, 2009.

[5] Rueda, S., King, D.H., and Jaeger, T., “Verifying compliance of trusted programs,” *Proceedings of the 17th USENIX Security Symposium*, pages 321-334, August 2008.

[6] Rieh, S. Y., Danielson, D. R. (2007). Credibility: A multidisciplinary framework. In B. Cronin (Ed.), *Annual Review of Information Science and Technology* (Vol. 41, pp. 307-364). Medford, NJ: Information Today.

[7] Traynor, P., Kumar, R., Bin Saad, H., Cao G., and La Porta, T.F., “Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks,” IEEE Transactions on Mobile Computing, 6(6):663-677.

[8] Cao, G. “A sacalable low-latency cache invalidation strategy for mobile environments,” in IEEE Transactions on Knowledge and Data Engineering, vol. 15, 2003.

[9] He, X., and Yener, Y., “A New Outer Bound for the Secrecy Capacity Region of the Gaussian Two-Way Wiretap Channel,” Proceedings of the IEEE International Conference on Communications, ICC'10, Cape Town, South Africa, May 2010.