On Detection and Concealment of Critical Roles in Tactical Wireless Networks

Zhuo Lu
University of Memphis,
Email: zhuo.lu@memphis.edu.

Cliff Wang
Army Research Office,
Email: cliff.wang@us.army.mil.

Mingkui Wei
NC State University,
Email: mwei2@ncsu.edu.

***Abstract*—In tactical wireless networks, the one-to-multiple communication model is pervasive due to commanding and control requirements in mission operations. In such networks, the roles of nodes are non-homogeneous; i.e., they are not equally important. This, however, opens a door for an adversary to target important nodes in the network by identifying their roles. In this paper, we investigate an important open question: *how to detect and conceal the roles of nodes in tactical wireless networks?* Answers to this question are of essential importance to understand how to identify critical roles and prevent them from being the primary targets. We demonstrate via analysis and simulations that it is feasible and even accurate to identify critical roles of nodes by looking at network traffic patterns. To provide countermeasures against role detection, we propose role concealment methods based on proactive network strategies. We use simulations to evaluate the effectiveness and costs of the role concealment methods.**

I. Introduction

Tactical wireless networks [1]–[3] are mission-critical mobile ad-hoc networks that involve unique challenges due to tactical requirements, such as reliability and security in hostile environments. Tactical wireless networks are envisioned to provide the most effective solutions to cyber dominance for networked warfighters.

In tactical wireless networks, the roles of nodes are non-homogenous; i.e., they are not equally important. For example [4], Intelligence, surveillance, and reconnaissance (ISR) operations are used to collect operational information, such as status of the enemy, terrain, and weather. Such information will be delivered to the commander, who will make the best judgement to task ISR assets and soldiers. Therefore, commanding and control roles are pervasive in tactical wireless networks. At the network level, such roles lead to the one-to-multiple communication model in the network, which is usually facilitated by either unicast or multicast protocols [5]–[7].

In this paper, we investigate an important question: *how to detect and conceal the roles of nodes in tactical wireless networks?* This question has not been well explored in the literature, but is of essential importance. In particular, we say that a node has a commanding role in a tactical network if the number of its active network flows with other nodes exceeds a given threshold and say that it has an acting role otherwise. In this paper, the concept of a node being commanding does not necessarily mean that the node is sending real operational commands to others, but indicates that it is actively interacting with others, thereby playing an important role in the network by definition. Accordingly, the problem becomes two-fold: 1) the role detection problem, i.e., whether we can accurately identify such critical commanding nodes in a network from an adversary's point of view; and 2) the role concealment problem, i.e., whether we can protect such nodes from being identified from a defender's points of view.

The role detection and concealment problems seem to be an endless arms race. As both role detection and concealment are not well investigated in the literature, in this paper, we attempt to provide an initial study on both problems. More specifically, we first show that network flow analysis [8]–[15] servers as a foundation for role detection, based on which we develop our role detection method. Simulation results demonstrate that it is quite feasible and accurate to identify the roles of commanding nodes. These nodes can become an adversary's primary targets, thus must be protected by role concealment methods. Accordingly, we propose a line of network strategies, which proactively cause network traffic dynamics to counter network flow analysis based role detection. We also use simulations to evaluate the performance and cost of such proactive strategies.

Our contributions are two-fold: 1) we provide an initial study on role detection and concealment, which are important in tactical wireless networks; 2) we propose role detection and concealment methods and comprehensively evaluate their performance. Our initial work demonstrates that it is vital to be proactive to protect critical nodes from being identified and becoming primary targets in tactical wireless networks.

The rest of this paper is organized as follows. In Section II, we introduce models and state the problem. In Sections III and IV, we present our findings in role detection and concealment, respectively. Finally, we conclude in Section V.

II. Models and Problem Statement

In this section, we introduce models and state the problems of role detection and concealment. Notations: We denote by $\mathbf{A}^T$ the transpose of matrix $\mathbf{A}$. We use $\mathbb{R}^{n\times m}$ to represent the set of all n-by-m real-valued matrices.

A. Network Model and Roles of Nodes

We consider a tactical wireless network with n nodes (indexed by $\mathcal{N} = \{1, 2, \cdots, n\}$) distributed independently and uniformly on region $\Omega = [0, \sqrt{n/\lambda}]^2$ for a large node density

This research in this paper is supported by NSF CNS-1464114.

λ such that the network is connected (asymptotically almost surely) [16]. We say two nodes have a network link if they are in each other's transmission range r.

To meet tactical requirements, such as information collecting and reporting, we define that there are two roles in the network: *commanding* and *acting* in the following.

Definition 1 (Commanding and Acting Roles): We say a node is *commanding* if it has network flows with rates in rate region Σ to/from at least n_c nodes (where $n_c > 1$ is said to be the threshold for commanding); and say it is *acting* otherwise. Mathematically, we define that the role of node i ($i \in \mathcal{N}$), denoted by R_i, has value 1 if it is commanding, and value 0 otherwise; i.e.,

$$R_i = \begin{cases} 1 & \text{if node } i \text{ is commanding,} \\ 0 & \text{if node } i \text{ is acting,} \end{cases}$$

for $i \in \mathcal{N}$.

Then, we define a role vector $\mathbf{R} = [R_1, R_2, \cdots, R_n]^T$. Accordingly, the roles of all nodes can be characterized by the role vector $\mathbf{R}$ in the network. We note that $\mathbf{R}$ contains important, sensitive information in the network and should never be revealed. If $\mathbf{R}$ is disclosed, an adversary can immediately know which node plays an important (commanding) role in the tactical network.

It is worth noting that the rate region Σ is a set of allowed rates. It can be a generic region, such as $[\sigma, +\infty)$ to take into account any network flow as long as the flow rate is larger than a threshold σ. It can also be a specific region, such as $[\sigma - \epsilon, \sigma + \epsilon]$ to only consider network flows generated by a military standard with a fix communication rate σ, where ϵ is the allowed error margin.

B. Adversary Model

We assume a relatively strong attacker existing in the network. The goal of the attacker is to successfully detect the role of each node in the network; i.e., decide whether a node is commanding or acting. The attacker can overhear the data transmissions on each link and estimate the transmission rate at each link (e.g., by placing eavesdroppers all over the network). The attacker is aware of the network topology; hence, given a routing protocol used in the network (e.g., shortest path routing), the attacker knows the routing path between any source-destination pair.

The attacker will observe the network for a sufficiently-long observation period; then attempt to detect the role of each node. In this paper, the role detection and concealment methods, and their associated operations will all happen within this observation period, unless otherwise specified.

C. Problem Statement

Given the network, role and adversary models, we state our research problems.

Definition 2 (Role Detection): The goal of the adversary is (by observing network traffic transmissions) to find a role vector estimate $\hat{\mathbf{R}}$ such that $\hat{\mathbf{R}}$ is in close value to the real role vector $\mathbf{R}$. In the best case, $\|\hat{\mathbf{R}} - \mathbf{R}\|$ should be minimized.

Definition 3 (Role Concealment): The goal of the network defender is to make the real role vector $\mathbf{R}$ difficult to detect. In the best case, for any node i, the adversary's estimate $\hat{R}_i$ in $\hat{\mathbf{R}}$ should be equal to real value R_i in $\mathbf{R}$ with probability 0.5 (i.e., equivalent to a random 0/1 guess).

Note that it seems that the two research problems become an endless arms race: a concealment method can be developed based on attacking a role detection method, and vice versa. As both role detection and concealment are not well studied in the literature, we aim to propose an initial study on the two problems. In particular, we first show that the state-of-the-art on network flow analysis makes it feasible to detect node roles in a network, then exploit proactive design of countermeasures to conceal node roles, which leads to substantial difficulty for any role detection based on network flow analysis.

III. Role Detection

In this section, we describe our design of role detection methods based on network flow analysis. We first introduce the backgrounds on network flow analysis, then design our methods, and finally use simulations to show the effectiveness of our method.

A. Backgrounds on Network Flow Analysis

According to our definitions, the role R_i of node i is based on the number of its network flows to other nodes. Therefore, our design of role detection must be based on network flow analysis, i.e., estimating the rates of all possible flows in the network. Recent advances in network flow analysis have already established a research line called network tomography, which is an effective way to infer end-to-end flow or link rates from network measurements [8]–[14]. Thus, it is necessary to briefly introduce network tomography before moving to the design of network flow analysis based on role detection.

In the network with n nodes, there are at most $\frac{n(n-1)}{2}$ undirected flows[1]. All of them are associated with a flow rate vector $\mathbf{x} \in \mathbb{R}^{\frac{n(n-1)}{2} \times 1}$, whose entry represents the rate of each flow. The attacker aims to get an estimate $\hat{\mathbf{x}}$ in close value to $\mathbf{x}$. However, the attacker cannot directly see $\mathbf{x}$, but can only observe the data transmission on each link. Therefore, the attacker has to estimate the flow rate vector from a link rate vector, which belongs to network tomography. In particular, the objective of the attacker is to compute an estimate of $\mathbf{x} \in \mathbb{R}^{\frac{n(n-1)}{2} \times 1}$ from the observed link rate vector $\mathbf{y} \in \mathbb{R}^{L \times 1}$, where L is the number of point-to-point links in the network. Each entry of $\mathbf{y}$ is the data transmission rate at each link.

It has been shown in the literature (e.g., [8], [10], [12], [13]) that $\mathbf{x}$ and $\mathbf{y}$ exhibit a linear relationship, i.e.,

$$\mathbf{y} = \mathbf{A}\mathbf{x}, \tag{1}$$

where $\mathbf{A} = \{a_{i,j}\}$ is called the routing matrix in the network, whose element $a_{i,j}$ has value 1 if the i-th link is on the routing path of flow j, and value 0 otherwise. Various methods have

[1]For the sake of notation simplicity, we consider undirected links in this paper. We note that the directed link case does not affect any formulation in this paper and thus is a straightforward extension.

been developed to solve (1) in an effective way (e.g., [8]–[11], [13], [17], [18]). In this section, we do not intend to develop any method to solve (1), but aim to leverage existing solutions to (1) for building a role detection method.

B. Detection Method Design

We design a detection method to detect the roles defined in Definition 1. As the role of a node is defined based on how many network flows it has, the method consists of two steps in the following.

1) Flow rate estimation. Use a network tomography method to estimate all rates of possible flows in the network, denoted by a vector $\hat{\mathbf{x}} = [\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_{\frac{n(n-1)}{2}}]^T$. The estimate $\hat{\mathbf{x}}$ should be in close value to $\mathbf{x}$.
2) Role detection. For each node i, estimate its role $\hat{R}_i$ as

$$\hat{R}_i = \mathbf{1}_{\left\{\left(\sum_{f \in \mathcal{F}_i} \mathbf{1}_{\{\hat{x}_f \in \Sigma_1\}}\right) \geq \sigma_2\right\}}, \quad (2)$$

where $\mathcal{F}_i$ denote the set of indexes of all network flows from/to node i, Σ_1 is the rate threshold range for flow detection, σ_2 is the threshold for role detection, and $\mathbf{1}_E(x)$ is the indicator function that has value 1 if event E happens and value 0 otherwise.

To be more specific, the second step in the role detection method is to first compute the number of network flows from/to node i with rate within the threshold range Σ_1, then compare the number with the threshold σ_2 to decide whether the role is commanding or acting. It is obvious that if the first step can estimate the rates of all possible network flows with small error, the second step will then accurately detect all roles. In the literature, there are a wide range of tomography methods available for the first step. In this paper, we use an efficient basis pursuit denoising method in [19].

C. Performance Evaluation

We use simulations to evaluate the effectiveness of the proposed role detection method. In our simulations, the transmission range of each node is normalized to 1. We generate a 100-node network with density 5 (i.e., there are on average 5 nodes in a unit area). All nodes are uniformly distributed in the network. There are 2 commanding nodes and 98 acting nodes in the network. Each commanding node is communicating with 10 other random nodes. Among all acting nodes, there are 10 random source-destination node pairs. The rate of each network flow is randomly distributed from 1 to 2 Mbps.

Fig. 1 shows a network topology in one simulation run. In Fig. 1, two commanding nodes are sources/nodes 1 and 2. Each commanding node has 10 network flows to other random destinations in the network. The links with active network traffic induced by these flows are shown in solid lines. Note that for better illustration, random network flows between acting noes are not shown in Fig. 1.

Given the network topology and flow setups in Fig. 1, we evaluate the performance of the role detection algorithm. In particular, we first show the performance of flow rate estimation, as it is the basis for role detection. We use a

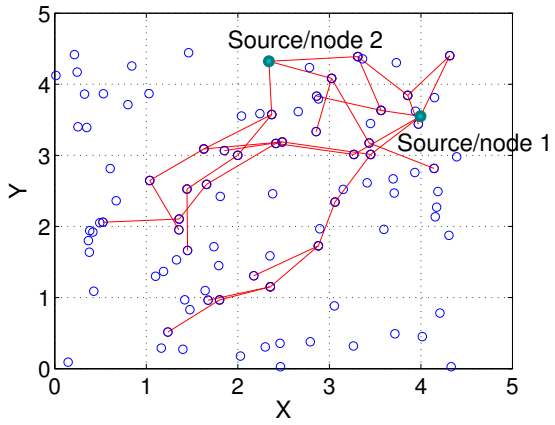

Fig. 1. Network topology and flows initiated by two commanding nodes (nodes 1 and 2) in the 2-D network region (wireless transmission range is normalized to 1).

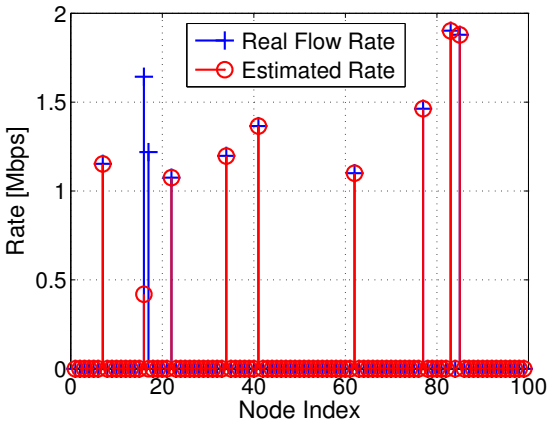

Fig. 2. Estimated flow rates from node 1 to nodes 2–100 in comparison to real flow rates.

basis pursuit denoising algorithm proposed in [19] for flow rate estimation. Fig. 2 depicts the comparison between estimated and real flow rates for commanding node 1 to all possible destinations (i.e., nodes 2 – 100). It is observed from Fig. 2 that among all ten flows of node 1, eight are accurately estimated, one has a substantial error, and the one is completely miss-detected. This indicates the following.

- Most of the flow rates can be accurately estimated, providing a good foundation for the next role detection step;
- The thresholds Σ_1 and σ_2 in role detection algorithm (2) should be properly set to achieve a good balance between detection ratio and false alarm.

Next, we run role detection based on the flow rate estimation with network setups in Fig. 1. We set $\Sigma_1 = [700, +\infty]$ (i.e., we want to detect all flows with rate no less than 700 Kbps) and $\sigma_2 = 7$. Table I shows the following four performance metrics.

- Flow detection error rate, which is the probability that the existence of a flow is not detected.

- Commanding role detection rate, which is the probability that a commanding node is indeed detected as a commanding node.
- Commanding role false alarm, which is the probability that an acting node is mistakenly detected as a commanding node.
- Overall role detection error rate, which is the probability that the role of a node (either commanding or acting) is correctly detected.

TABLE I
ROLE DETECTION PERFORMANCE.

Flow Detection Error Rate:	1.4%
Commanding Role Detection Rate:	100%
Commanding Role False Alarm:	0%
Overall Role Detection Error Rate:	0%

We see from Table I that the flow detection error rate is 1.4%, indicating that most network flows can be identified in the network with rate threshold region $\Sigma_1 = [700, +\infty]$. Commanding role detection rate and false alarm are very important metrics for detecting critical roles in tactical wireless networks. As most of the time, the adversary may be only interested in these important nodes and consider them as the primary targets. We see that the role detection method can detect these roles with 100% accuracy and 0% false alarm for the network setups in Fig. 1. And the overall role detection error rate is also 0% shown in Table I.

Results from Table I are obtained from one simulation run with a particular network topology. Therefore, we also comprehensively evaluate the role detection performance by averaging 100 random network topologies, each of which also includes randomly generated network flows, commanding and acting nodes.

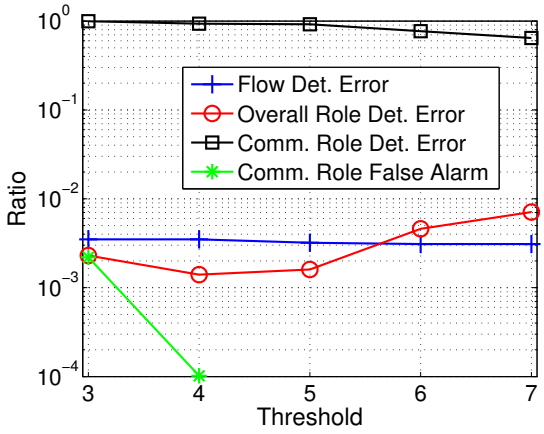

Fig. 3. The performance metrics of role detection for different threshold σ_2 (from 3 to 7).

In all simulation runs, we set $\Sigma_1 = [700, \infty]$ and vary the value of σ_2 from 3 to 7 in the network. Fig. 3 shows the performance of the role detection method. We can observe from Fig. 3 that as the threshold increases, the commanding role detection rate decreases; at the same time, the commanding role false alarm also decreases. This is intuitively true because a higher threshold means a tougher detection standard, which decreases the detection ratio and false alarm at the same time. From Fig. 3, it is observed that around 50% of n_c is a good threshold to achieve good performance in commanding role detection. Note that this can also depend on conditions in applications, such as how many network flows usually a command node has.

In summary, our simulations show that role detection is not only feasible but also accurate, which poses a challenging issue against protecting critical nodes from being exposed in tactical wireless networks.

IV. ROLE CONCEALMENT

A. Design Methodology

We have shown the feasibility and effectiveness of the proposed role detection method in the previous section. From a network defender's perspective, it is critical to design strategies to make sure that an adversary can conclude nothing or wrong information from role detection, which we call *role concealment*. It has a great potential to be deployed in tactical wireless networks where role detection must be prevented.

Nonetheless, an adversary can perform role detection via only passive observation or overhearing, which means that the presence of the adversary may be never correctly known. Therefore, role concealment should be proactive (i.e., always actively online) rather than following a wait-and-detect-then-act paradigm.

To systemically develop proactive strategies for role concealment, a natural starting point is to take a close look at the role detection process, then attempt to break its underlying conditions to make it not work. Apparently, role detection is based on network flow detection. Therefore, we first need to understand how network flow detection works. Fig. 4(a) shows an illustrative example of how flow detection works: node A has an end-to-end flow with rate 100kbps to node H and node B also has a flow with rate 50kbps to node H. Suppose that there is an adversary that attempts to use flow analysis to deduce from all link observations the facts that nodes A and B have 100kbps and 50kbps flows to node H, respectively. If the adversary is aware of routing paths and overhears all link transmissions, i.e., A→C: 100kbps, C→F: 100kbps, B→D: 50kbps, D→F: 50kbps, and F→H: 150kbps (because two flows use the same F→H link). It is easy to use a method to get the facts: A→H is 100kbps, B→H is 50bps, and there is no other flow in the network.

There are two conditions that a flow analysis method relies on to successfully deduce the facts of A→H and B→H. (i) The reason that the adversary observes link transmissions is only because there exist some end-to-end flows in the network. In other words, if there is no network flow, no data transmission should be observed. (ii) The adversary is aware of how data is routed from a source to a destination, which is determined by the routing protocol used in the network.

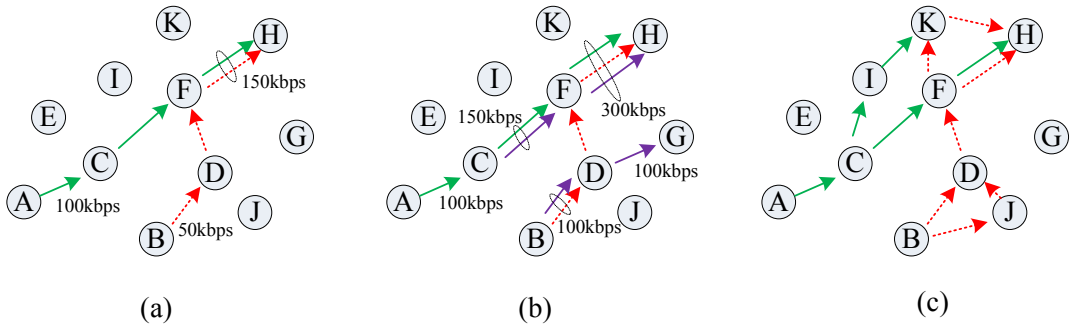

Fig. 4. Simple examples of proactive strategies: (a) normal network operation, (b) transmitting deception traffic, and (c) changing routing strategies.

Both conditions usually hold in a network because optimized data transmission and routing mechanisms are widely used in a network. As one major objective in network design is to optimize the performance (e.g., maximizing the throughput or minimizing the delay), it is apparent that nodes should not transmit anything if they have no data to transmit or forward. In addition, a routing path should always be optimized from a source to a destination. Such design can lead to static or predictable routing paths, which can be in turn taken advantage of by the adversary to infer information.

Accordingly, in order to make flow analysis inaccurate, strategy design should be focused on breaking the two conditions that it depends on.

- Transmitting redundant traffic into the network to break condition (i). We call such traffic *deception traffic*. In this case, the link observations are due to either deception traffic or real network flows. For example, as shown in Fig. 4(b), nodes B, C, D, and F all transmit an amount of deception traffic into the network, which acts like camouflage over the real network flows. Thus, it becomes difficult for the adversary to infer the real network flow information.
- Keeping changing routing to break condition (ii). We call such a strategy *routing changing*. For example, as shown in Fig. 4(c), if nodes A and B no longer use the static routing paths, but vary their paths to node H, it is difficult for the adversary to correctly acquire the exact routing path information that varies over time.

Both deception traffic and routing changing strategies are proactive and can cause more dynamics in the network to make flow analysis inaccurate, and accordingly failing role detection. On the other hand, however, they also break the requirement of the optimized network design (e.g., not always choosing the optimal routing path), thereby resulting in potential performance loss. A key question is under limited costs, what we can do for role concealment.

In this paper, our objective is to design these two proactive strategies with the simplest form to avoid incurring substantial operational complexity in an already complicated network environment. Thus, we consider a deception traffic strategy, in which each node transmits deception traffic independently to its one-hop neighbor. The amount of deception traffic on each link is always bounded above such that the performance degradation is also limited. We consider a routing changing strategy, in which each node will randomly select a different (longer) path for data delivery to a destination.

B. Simulations

We use simulations to evaluate the effectiveness and cost of role concealment methods. We generate a similar 100-node network with density 5. All nodes are uniformly distributed in the network. There are 2 commanding nodes and 98 acting nodes in the network. The rate of each network flow is randomly distributed from 1 to 2 Mbps. There exists an adversary that attempts to use the role detection method discussed in Section III to detect the role of each node in the network.

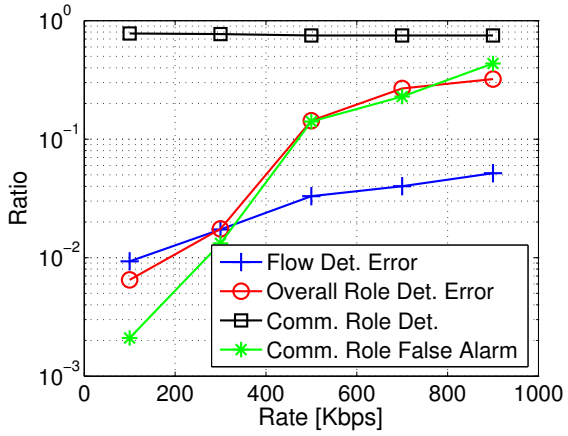

Fig. 5. The performance metrics of role detection under the deception traffic based role concealment method.

We first evaluate the performance of the deception traffic strategy. The deception traffic rate on each link is uniformly distributed from 0 to a given rate. Fig. 5 shows the performance metrics of role detection affected by deception traffic with limited average traffic rate from 100–900 Kbps. We can see from Fig. 5 that as the deception traffic rate increases, the commanding role detection ratio decreases and approximately remains at 75.0%; and the commanding role false alarm increases sharply to 43.5%. This means that deception traffic significantly reduces the performance of role detection, particularly increasing false alarm as all nodes are transmitting

in the network (so they are very likely to be considered as commanding). It is obvious that the overhead cause by deception traffic is large as it requires every node to transmit in the network.

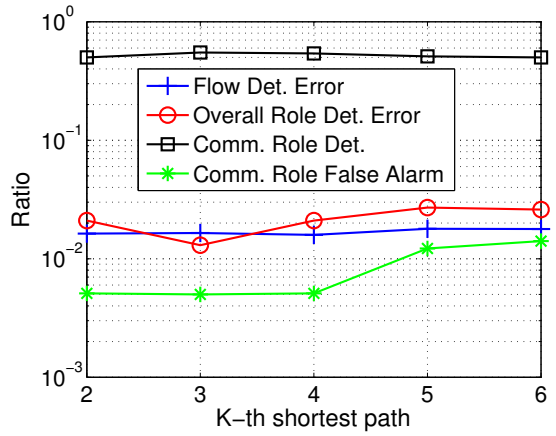

Fig. 6. The performance metrics of role detection under the routing changing based role concealment method.

We then evaluate the performance of the routing changing strategy. Each node will use K-th shortest path routing for data delivery ($K \geq 2$); however, we assume that the adversary has no such knowledge and thinks everyone still uses the (1st) shortest path. This, obviously, will lead to routing information mismatch in role detection. Fig. 6 shows the performance metrics of role detection affected by routing changing with $K = 2, 3, 4, 5, 6$. it is noted from Fig. 5 that as long as $K \geq 2$, the commanding role detection ratio is approximately 50.0%, which indicates that commanding role detection now becomes a random 0/1 guess; and the commanding role false alarm increases slightly to 1.41%, which is much smaller compared with the false alarm induced by deception traffic in Fig. 5. This is because when using routing changing, no node will transmit redundant traffic (so they are less likely to be considered having more network flows). The role detection error is due to information mismatch.

In addition, we also measure the delay performance degradation due to routing changing as each node will use a longer routing path, causing more delivery delay. Table II shows the delay cost for $K = 2, 3, 4, 5, 6$. For example, $K = 6$ will cause 12.2% more delay in average message delivery in the network.

TABLE II
DELAY PERFORMANCE DEGRADATION.

K:	2	3	4	5	6
Degradation:	5.56%	7.92%	9.37%	10.9%	12.2%

C. Discussions

From our simulations, we can see that deception traffic is effective in causing false alarm in role detection, but requires all network nodes transmitting deception traffic, causing throughput degradation in the network. Routing changing is a good strategy to counter the commanding role detection at the cost of the delay performance. They can be chosen based on different application requirements and conditions in tactical wireless networks. We note that more sophisticated strategies can be developed upon the deception traffic and routing changing strategies discussed in this paper.

V. CONCLUSIONS

In this paper, we studied the role detection and concealment problems. We showed that our role detection methods can identify critical roles of nodes. Then, we proposed two proactive strategies (deception traffic and routing changing) for role concealment, and use simulations to show the effectiveness and cost of the proposed strategies. Our work demonstrated that it is vital to be proactive to protect critical nodes from being identified in tactical wireless networks.

REFERENCES

[1] S. H. Lee, S. Lee, H. Song, and H. S. Lee, "Wireless sensor network design for tactical military applications: remote large-scale environments," in *Proc. of MILCOM*, 2009, pp. 1–7.

[2] G. F. Elmasry, C. J. McCann, and R. Welsh, "Partitioning QoS management for secure tactical wireless ad hoc networks," *IEEE Communications Magazine*, vol. 43, no. 11, pp. 116–123, 2005.

[3] G. F. Elmasry, "A comparative review of commercial vs. tactical wireless networks," *IEEE Communications Magazine*, vol. 48, no. 10, pp. 54–59, 2010.

[4] A. Bar-Noy, G. Cirincione, R. Govindan, S. Krishnamurthy, T. LaPorta, P. Mohapatra, M. Neely, and A. Yener, "Quality-of-information aware networking for tactical military networks," in *Proc. of IEEE PERCOM Workshops*, 2011, pp. 2–7.

[5] T. Kunz and L. Li, "Robust broadcasting in tactical networks using network coding," in *Proc. of MILCOM*, Oct 2014, pp. 1213–1222.

[6] ——, "Broadcasting in multihop mobile tactical networks: To network code or not," in *Proc. of IWCMC*, 2010, pp. 676–680.

[7] D. Kidston and M. Shi, "A multicast routing technique for tactical networks," in *Proc. of MILCOM*, 2012, pp. 1–6.

[8] R. Castro, M. Coates, G. Liang, R. Nowak, and B. Yu, "Network tomography: Recent developments," *Statistical Science*, vol. 19, pp. 499–517, 2004.

[9] T. Bu, N. Duffield, F. L. Presti, and D. Towsley, "Network tomography on general topologies," in *Proc. of ACM SIGMETRICS*, 2002.

[10] J. D. Horton and A. Lopez-Ortiz, "On the number of distributed measurement points for network tomography," in *Proc. of ACM SIGCOMM IMC*, 2003, pp. 204–209.

[11] A. Soule, A. Lakhina, N. Taft, K. Papagiannaki, K. Salamatian, A. Nucci, M. Crovella, and C. Diot, "Traffic matrices: Balancing measurements, inference and modeling," in *Proc. of ACM SIGMETRICS*, 2005.

[12] H. Yao, S. Jaggi, and M. Chen, "Network coding tomography for network failures," in *Proc. of IEEE INFOCOM*, 2010.

[13] A. Chen, J. Cao, and T. Bu, "Network tomography: Identifiability and fourier domain estimation," *IEEE Trans. Signal Processing*, vol. 58, pp. 6029–6039, 2010.

[14] Q. Zhao, Z. Ge, J. Wang, and J. Xu, "Robust traffic matrix estimation with imperfect information: Making use of multiple data sources," in *Proc. of ACM SIGMETRICS*, 2006, pp. 133–144.

[15] Z. Lu and C. Wang, "Network anti-inference: A fundamental perspective on proactive strategies to counter flow inference," in *Proc. of IEEE INFOCOM*, Apr. 2015.

[16] M. Penrose, *Random Geometric Graphs*. Oxford Univ. Press, 2003.

[17] E. Candes, J. Romberg, and T. Tao, "Stable signal recovery from incomplete and inaccurate information," *Communications on Pure and Applied Mathematics*, pp. 1207–1233, 2005.

[18] ——, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *IEEE Trans. Information Theory*, vol. 52, pp. 489–509, 2006.

[19] M. P. Friedlander and M. A. Saunders, "Active-set methods for basis pursuit," in *Proc. of WCOM*, 2008.