

Missing and Spurious Interactions in Heterogeneous Military Networks

Changjun Fan^(✉), Zhong Liu, Baoxin Xiu, and Lianfei Yu

Science and Technology on Information Systems Engineering Laboratory,
National University of Defense Technology, Changsha, Hunan 410073, China
fanchangjun09@163.com

Abstract. As we all know, decision-makers need the high quality battlefield information to design the best operation plans, however, real intelligence data are often incomplete and noisy, where missing links prediction methods and spurious links identification algorithms can be applied. Military organizations could be modeled as heterogeneous complex networks, where nodes represent different types of functional units and edges denote different types of communication links. In this paper, we proposed a combined link prediction index considering both the nodes' types effects and their structural similarities, and demonstrated that it is remarkably superior to all the 25 existing similarity-based methods both in predicting missing links and identifying spurious links in a real military network data; we also investigated the algorithms' robustness under noisy environment, and showed our method maintained the best performance under the condition of small noise. In the end, as the FINC-E model, here used to describe the heterogeneous military organizations, is also suitable to many other social organizations, such as criminal networks, business organizations, etc., thus our method has its prospects in these areas for many tasks, like detecting the underground relationships between terrorists, predicting the potential business markets for decision-makers, and so on.

Keywords: Complex military organization · Link prediction · FINC-E model · Social organization

1 Introduction

The state-of-art complex military organization named “System of System, SOS” has been playing an increasingly significant role in nowadays’ warfare, disaster response, nation building, peace operations and counter-terrorism [10] with the rapid development of information technology and military science. Modeling complex military organization is a challenging task, and there are some inspiring works [1–3] in this field, and the most successful one is the FINC model proposed by Dekker [4–7], and Guoli Yang extended it as the FINC-E model [20].

Electronic supplementary material The online version of this chapter ([doi:10.1007/978-981-10-2993-6_2](https://doi.org/10.1007/978-981-10-2993-6_2)) contains supplementary material, which is available to authorized users.

FINC(Force, Intelligence, Networking and C2) methodology classified the nodes into three types: C2 node(C2), like command post, control center, etc., Intelligence node(I), like radar, AWACS, etc., and Force node(F), like missile position; and links provide communications between nodes, indicated by lines or arrows, depending on whether information flow is bidirectional or unidirectional. In FINC-E model, there are five types of links, Intelligence link($I \rightarrow C2$, unidirectional), C2 link($C2 - C2$, bidirectional), Fire link($I - > F$, unidirectional), Decision link($C2 - F$, bidirectional) and Communication link(I-I, bidirectional). Each node has many attributes, like attack cost, InEdge, OutEdge, etc., each link also has attributes, such as information transfer delay, information load, information accuracy, attack cost, InNode, OutNode, etc. More details see in [20]. In this paper, FINC-E model is utilized to model the heterogeneous military organization.

As for the problem of link prediction, it attempts to estimate the likelihood of the existence of links between nodes based on the attributes of nodes as well as the structure of networks [8, 13, 14]. Due to its formal simplicity, theoretical value and practical significance, link prediction has attracted increasing attentions from various researches and engineers, such as physicists, mathematicians, computer scientists, statisticians, biologists, etc. As for complex military organization, link prediction may be more significant, since the war determines a country of vital significance, and quality of intelligence is critical to military decisions, as a formal representation of military intelligence, network topology for complex military organization has to be true enough to guarantee the reliability of the subsequent analysis, such as critical operational units analysis, community analysis, network evolving analysis, etc. However, due to the complex battle field situations and the expensive costs of military intelligence collection, it is nearly impossible to obtain an absolute accurate military network, there must be some missing information or spurious noise, in other words, missing links and spurious links in network topology. If we can predict them or identify them in advance with link prediction methods, it would be both meaningful to optimize the military organization structure for our side and attack the other side's critical operational components, which are sure to enhance the accuracy of military decisions and accelerate the process of victory.

Current link prediction methods are mainly designed basing on the definition of node similarity, which assumes that the greater the similarity values between nodes are, the higher the likelihood of the existence of links between them [15]. Another branch is based on the network structure only, which is named structural similarity, and can be further divided into three types: local information based similarity, such as CN index; path-based similarity, such as Katz index; random walk-based similarity, such as ACT index. There are 25 main similarity indexes now, details about them see in SI. And they are utilized to compare the prediction accuracy with the method proposed in this paper. However, all the existing methods may not work well in complex military network, for these methods are only designed for homogeneous networks, but linking behaviors are different between different types of nodes, for example, if there are command nodes and intelligence nodes densely connected in a control-centered military organization, intelligence nodes are more likely to build links with commands nodes

than forces nodes. As a result, an index combining this impact and traditional topological similarity is proposed in this paper to improve the link prediction accuracy in complex military organization network.

The major contributions of this study are summarized as follows:

1. For the first time, we quantify the nodes' types effect on their linking behaviors, and empirically proved that it could remarkably improve the prediction accuracy of all the current methods;
2. We design a new link prediction index for heterogeneous military network and it is superior to all the other methods both in missing links prediction and spurious links identification tasks;
3. We investigate the algorithms' robustness under noisy environment, and demonstrate that our method maintains the best performance under the condition of small noise, and we also observe that spurious links are more destructive than missing links in military networks, which is just opposite to that in recommendation systems.

The remainder of this paper is organized as: Sect. 2 describes the methodology in detail, Sect. 3 conducts experiments on a real military network data and compared the performance of our method with all the other methods, Sect. 4 concludes the paper and pointed the further directions.

2 Methodology

Complex military organization can be described as $G(V, E, A, L, W)$ in FINC-E model, where V denotes operation units, E indicates communication links between nodes, A is a set of node types, L represents link types, mainly refers to five types. W is a set of weights, including node weights, like attack costs, and link weight, such as information loads. Just as mentioned in Introduction section, due to the complex battlefield situations and expensive costs of intelligence collection, there are often filled with noisy or incomplete information in the observations, which are reflected as spurious links or missing links respectively in the military network.

To purify the network topology, we used link prediction methods to predicting the missing links and identifying the spurious links based on the known network topology and nodes types information.

For the missing link prediction, the task is to estimate the existence tendency of all the non-observed links, and find the most possible non-observed ones. To test the algorithms' accuracy, the observed links, E , is randomly divided into two parts: the training set, E^T is treated as known information, while the probe set, E^P is used for testing. Obviously, $E^T \cup E^P = E$, $E^T \cap E^P = \emptyset$.

For spurious link identification, the task is to evaluate the reliability of all the observed links, and identify the most spurious links. To test the algorithm's accuracy, we randomly add some nonexistent links which constitutes the probe set E^P , and the given network (true network) together with the probe set constitute the training set E^T . Clearly, $E^T - E^P = E$, $E^T \cap E^P = E^P$.

Traditional methods for predicting missing links and identifying spurious links can be roughly divided into two classes: the probabilistic models and the similarity based algorithms: the former usually requires much information about node attributes, in addition to the observed network topology; the latter assigns a similarity score to every pair of nodes and ranks all links according to their scores. Since it is always very hard to collect enough nodes attributes, similarity based algorithms are thus the practical option, how to define the similarity between nodes is the key point for similarity algorithms, here we proposed the *LR* (Link Reliability) index, combining both the nodes' types information and their structural similarities.

2.1 Design of *LR*(Link Reliability) Index

Consider a complex military organization network $G(V, E, A, L, W)$, it is a heterogeneous directed weighted network, and it's difficult to directly conduct link prediction tasks, here we simplified it just a heterogeneous undirected unweighted network based on the following considerations: (1) link directions are totally determined by the two nodes linked, if two nodes' types are known, links between them are determined; (2) weights are often hard to obtain, and they have no obvious effects on linking behaviors between nodes. As a result, in this paper, link prediction is actually conducted in the network $\hat{G}(V, E, A)$, and our index, named Link Reliability (*LR*) is designed for it.

As we analyzed before, whether two nodes in the military network have links or not depends on two parts, one is the two linked nodes' types, denoted as T , the other is these two nodes' topological similarity, denoted as S . Let R stands for the link reliability, then we may have the following:

$$R = f(T, S) \quad (1)$$

f is the combined function of these two parts' effects.

Next, we deduce the forms of effect of nodes' types T , effect of node structural similarity S and the combined function f .

Effect of Nodes' Types. There are three types of nodes in the military network, and linking behaviors between different types of nodes are different. Here, the stochastic block model is utilized to give the mathematical formula of it. The stochastic block model is a general network model [11], it divides the nodes in the network into several groups, and the existence tendency between nodes is determined by the groups they belong to, nodes in the same group have the same linking behaviors. The model is most suitable for the situations where nodes' types significantly affect their linking behaviors, which is just the case this paper is to address.

A stochastic block model is composed of two parts: one is all the possible group division strategies, denoted as Ω ; the other is the linking probability matrix between different groups, denoted as Q . Given a specific block division P and the corresponding linking probability matrix Q , a stochastic block model $M = (P, Q)$

is then determined. The observed network A^O could be regarded as one from an unknown stochastic block model, let Ψ be a certain network property, then it is easy to obtain the following based on Bayes theorem:

$$p(\psi|A^O) = \int_{\Theta} p(\psi|M)p(M|A^O)dM \quad (2)$$

where Θ stands for all possible stochastic block models, and since $p(M|A^O)p(A^O) = p(A^O|M)p(M)$, formula (2) could be rewritten as:

$$p(\psi|A^O) = \frac{\int_{\Theta} p(\psi|M)p(A^O|M)p(M)dM}{\int_{\Theta} p(A^O|M')p(M')dM'} \quad (3)$$

Let Ψ be $A_{xy} = 1$, then $p(\Psi|A^O) = p(A_{xy} = 1|A^O)$ represents the linking reliability of node pair v_x, v_y based on the observed network A^O . Now we can obtain the form of T by proving the following theorem 1. Detailed proof sees the SI.

Theorem 1. *Given a complex military organization network $G(V, E, A)$, let σ_x denotes the type of node v_x , σ_y denotes the type of node v_y , and r_{σ_x, σ_y} is the number of all possible links between these two types of nodes. l_{σ_x, σ_y}^O represents the observed links between these two types nodes. Then the linking reliability for node pairs $\{v_x, v_y\}$ could be calculated as:*

$$p(A_{xy} = 1|A^O) = \frac{l_{\sigma_x, \sigma_y}^O + 1}{r_{\sigma_x, \sigma_y} + 2} \quad (4)$$

Therefore, formula of T is represented as $T(v_x, v_y) = p(A_{xy} = 1|A^O) = \frac{l_{\sigma_x, \sigma_y}^O + 1}{r_{\sigma_x, \sigma_y} + 2}$.

Effect of Nodes' Structural Similarity. Military network is a sparse network, where there are abundant nodes while with a few links, this may be the result of the hidden hierarchical structure in military organization. In [14], some random walk based indices, such as RWR , SRW , have been empirically demonstrated to be superior to the other methods on sparse networks, like the Power network and the Router network. As a result, we utilize the RWR indice, which obtained the best performance among all random walk based methods [14], to measure the effect of nodes' structural similarity in the military network.

Consider a random walker starting from node v_x , who will iteratively move to a random neighbor with probability c and return to v_x with probability $1 - c$. Denote $\vec{q}_x$ as the steady state of this random walker from node v_x , we have:

$$\vec{q}_x = cP^T \vec{q}_x + (1 - c)\vec{e}_x \quad (5)$$

where P is the transition matrix with $P_{xy} = 1/k_x$ if v_x and v_y are connected, and $P_{xy} = 0$ otherwise, $\vec{e}_x$ is the vector with x th element equals 1, and the left elements are all 0s. It can be obviously obtained as follows:

$$\vec{q}_x = (1 - c)(1 - cP^T)^{-1}\vec{e}_x \quad (6)$$

The RWR index is thus defined as

$$s_{xy}^{RWR} = q_{xy} + q_{yx} \quad (7)$$

where q_{xy} is the y th element of the vector $\vec{q}_x$. A fast algorithm to calculate this index was proposed by Tong et al. [19], and the application of this index to recommender systems can be found in Ref. [17].

Thus the formula of S is $S(v_x, v_y) = s_{xy}^{RWR} = q_{xy} + q_{yx}$.

Form the Combined Function f . Here we just utilize the simplest weighted average form to combine the two parts, which means the Link Reliability value could be calculated as:

$$R = f(T, S, \lambda) = \lambda T + (1 - \lambda)S = \lambda T(v_x, v_y) + (1 - \lambda)S(v_x, v_y) \quad (8)$$

And $R(v_x, v_y) = \lambda T(v_x, v_y) + (1 - \lambda)S(v_x, v_y)$, form of $T(v_x, v_y)$ and $S(v_x, v_y)$ see formula (4) and (7). Weight parameter λ is proportional to each part's prediction accuracy in specific cases. For instance, for a specific network A, if the first part's accuracy is T_A^{AUC} , the second part's accuracy is S_A^{AUC} , then we obtain:

$$\frac{\lambda}{1 - \lambda} \approx \frac{1 - f(T, S, 0)}{1 - f(T, S, 1)} = \frac{1 - S_A^{AUC}}{1 - T_A^{AUC}} \quad (9)$$

$$\text{Thus } \lambda \approx \frac{1 - S_A^{AUC}}{2 - (T_A^{AUC} + S_A^{AUC})}.$$

2.2 Evaluation Metrics

Two evaluation metrics adopted here are AUC (Area Under the receiver operating characteristic Curve)[9] and R [21]: AUC is used to measure the algorithms' accuracy in predicting missing links and identifying spurious links, and R is utilized to measure the ability for algorithms to maintain the prediction accuracies under noisy environments.

AUC . The AUC is a way to quantify the accuracy of prediction algorithms. Denote U as all the possible links in the network, E^T is the training set, E^P is the probe set. At each time, we randomly pick a missing link (i.e., a link in E^P) and a nonexistent link (i.e., a link in $U - E^T$) to compare their scores, if among n independent comparisons, there are n' times the missing link having a higher score and n'' times they have the same score, the AUC value for the missing links prediction task could be calculated as:

$$AUC = \frac{n' + 0.5n''}{n} \quad (10)$$

The above metric can also be used to quantify the performance on identifying spurious links.

If all the scores are randomly generated from an independent and identical distribution, the AUC values should be about 0.5. Therefore, the degree to which

the AUC value exceeds 0.5 indicates how better the algorithm performs than pure chance.

R. The R metric is recently proposed by Zhang et al. [21] to quantify to what extent the link prediction algorithms can resist the noise in the observed network.

$$R = \frac{1}{|L|} \sum_{q=0}^{|L|} \frac{AUC(q)}{AUC(0)} \quad (11)$$

where $L = ratio * |E^T|$, and $ratio$ is a quantity to measure the fraction of randomly added or deleted links. When $ratio$ is positive, $|ratio| * E^T$ links are randomly added to the training set, when $ratio$ is negative, $|ratio| * E^T$ links are randomly deleted from the training set. In order to keep the network connected, we cannot remove too many links, as a result, we keep $-0.3 \leq ratio \leq 1$, $AUC(q)$ is the AUC value of a link prediction method when q links are added ($ratio > 0$) to or deleted ($ratio < 0$) from the training set, when $ratio = 0$, $R = 1$.

3 Experiment Design and Result Analysis

In this paper, we provide a real military network, which is from an area's military organization (specific name is anonymized here due to the requirement of secret protections, but detailed network information is described in SI), it contains 89 entities, including 12 command nodes, 26 force nodes, and 51 intelligence nodes, and there are 150 observable links, including 30 Intelligence links, 16 Fire links, 26 Decision links, 51 Communication links and 17 $C2$ links. The topology of the network is drawn as Fig. 1.

3.1 Missing Links Prediction

Divide the network into two parts, the training set E^T contains 90% of the links, and the remaining 10% of links constitute the probe set E^P . It is obvious that $E^T + E^P = E$, and $E^T \cap E^P = \emptyset$. Compared our proposed method LR with all the other similarity-based indexes on the performance of AUC values. The prediction accuracies measured by AUC are shown in Fig. 2. Each data point is obtained by averaging over 1000 implementations with independently random divisions of the training set and the probe set. It is obvious from the comparisons that our method performs the best among all state-of-the-art algorithms (about 1.26% higher than the current best method), and its variance value is medium among all, indicating it is also a comparatively stable index.

3.2 Spurious Links Identification

Next we consider the identification of spurious links, where spurious links are those links being observed but not really existent, which may be resulted from

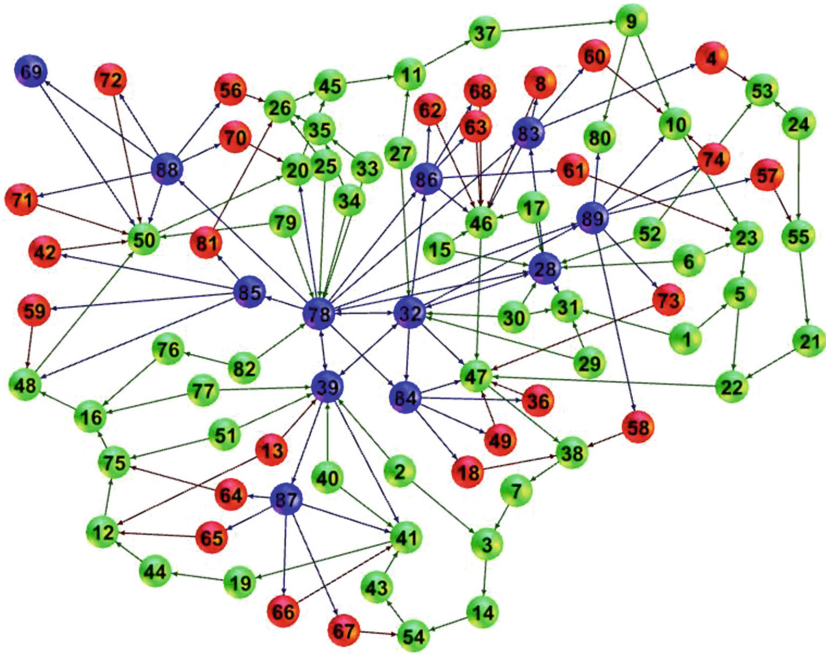


Fig. 1. Topology of the Network. Blue nodes represents the C2 units, like command posts, control center, etc., red nodes denotes the Force units, such as the missile position, and green nodes indicates the Intelligence units, like various optical stations, radar stations. (Color figure online)

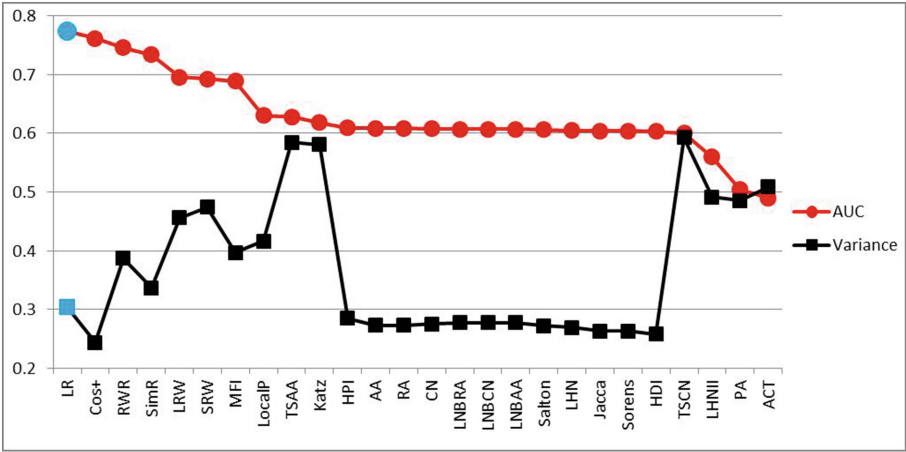


Fig. 2. Comparisons for the missing link prediction accuracy measured by *AUC*. Each data point is obtained by averaging over 1000 independent implementations, and the bold number emphasizes the highest value. The best parameters for some indexes are: *LR*(0.3), *Katz*(0.01), *LHNII*(0.9), *RWR*(0.95), *LRW*(5), *SRW*(5), *SimRank*(0.8).

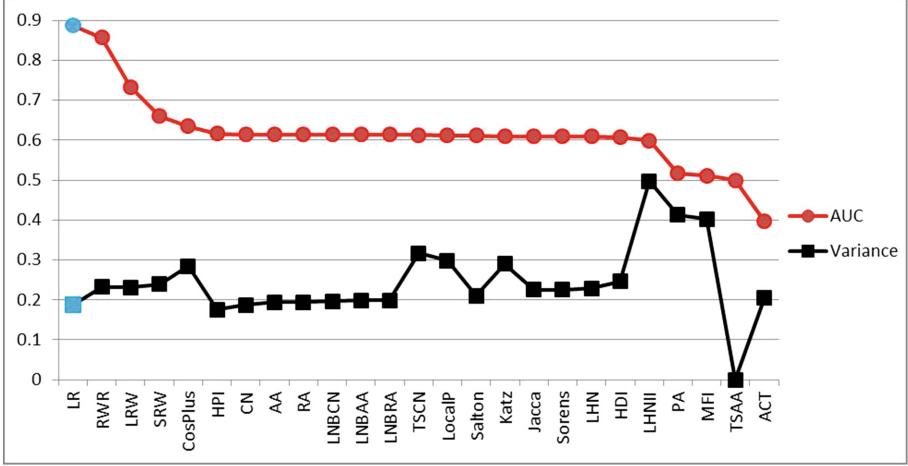


Fig. 3. Comparisons for the spurious link identification accuracy measured by *AUC*. Each data point is obtained by averaging over 1000 independent implementations, and the bold number emphasizes the highest value. The best parameters for some indexes are: *LR*(0.1), *Katz*(0.01), *LHNII*(0.9), *RWR*(0.95), *LRW*(5), *SRW*(5), *SimRank*(0.8).

experimental errors or data noise. To test the validity of the algorithms, we randomly add 10 % ($0.1|E|$) nonexistent links to the network data which constitute the probe set E^P , and the original network together with spurious links constitute the training set E^T . It is obvious that $E^T \cap E^P = E^P$, $E^T - E^P = E$. Compared *LR* with other methods on the performance of *AUC* values, results are shown in Fig. 3. Each data point is averaged over 1000 independent runs with different randomly generated spurious sets. Again, our method is remarkably better than all other state-of-the-art methods, specifically, 3.05 % higher than the current best method.

3.3 Combined Effectiveness with the Nodes' Types Effect T

It is claimed that nodes' types effect T index defined in formula (4) could well quantify the effects of nodes' types on their linking behaviors. Here, we empirically proved that all the existent methods have been enhanced on the accuracy if combined with T index, both in the missing links prediction task and the spurious links identification task, and the average rises are 8.39 % (Fig. 4) and 7.24 % (Fig. 5) respectively.

3.4 Algorithm Robustness

The training set is assumed to be entirely clean in the above tasks, however, in real cases, the reliability of the observed network data could not always be

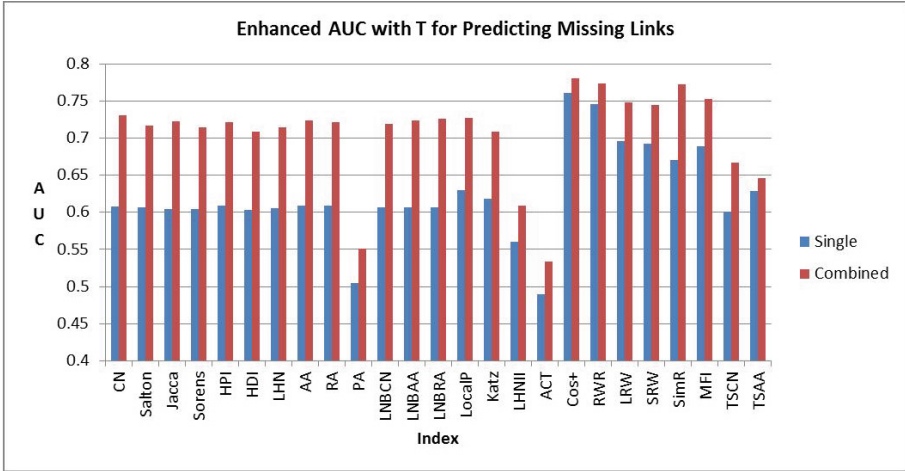


Fig. 4. Enhanced AUC with T for Predicting Missing Links. *Ratio* of the training set is 0.9, and each data point is averaged over 1000 independent implementations. The blue bars are prediction accuracies obtained by the current methods, the red bars are prediction accuracies obtained by current methods combined with T index. The best parameters for some indexes are: $LR(0.3)$, $Katz(0.01)$, $LHNII(0.9)$, $RWR(0.95)$, $LRW(5)$, $SRW(5)$, $SimRank(0.8)$. (Color figure online)

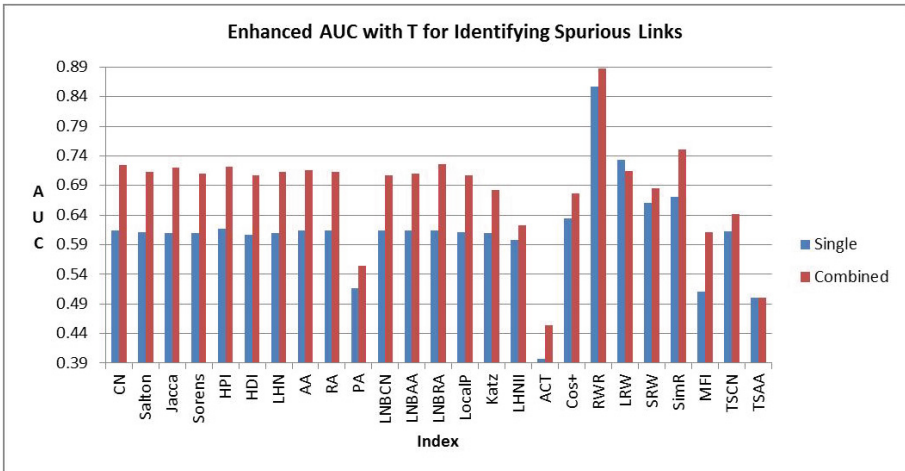


Fig. 5. Enhanced AUC with T for Identifying Spurious Links. *Ratio* of the training set is 0.9, and each point is averaged over 1000 independent implementations. The blue bars are accuracies obtained by the current methods, the red bars are accuracies obtained by current methods combined with T index. The best parameters for some indexes are: $LR(0.1)$, $Katz(0.01)$, $LHNII(0.9)$, $RWR(0.95)$, $LRW(5)$, $SRW(5)$, $SimRank(0.8)$. (Color figure online)

guaranteed, there is always filled with noisy or incomplete information in them, and that's exactly why the link prediction is so important. As a result, when applied to solve application problems, the link prediction methods will most likely work under noisy environment. This section, we investigate to which extent each link prediction algorithm can resist the noise.

In the experiment, after the network is divided into the training set E^T and probe set E^P , some links are randomly added to or deleted from E^T , let $ratio$ ranges from -0.3 to 1 .

In Fig. 6 we show effects of random noise on link prediction results. More precisely, we investigate the dependence of AUC on $|ratio|$. Since it is hardly to distinguish each of them if putting on all the 26 indexes together, we just select 4 typical ones ($LNBRA$ from local information based indexes, $LocalPath$ from global information based indexes, $Cos+$ from random walk based indexes), and compare them in Fig. 6.

It is observed that (1): AUC decreases with $|ratio|$ generally for most indexes, and AUC of different link prediction algorithms decays with $|ratio|$ with different speed. For example, LR has the highest AUC when $ratio = 0$, when $ratio = 100\%$, it reaches the lowest point among all. This indicates the performance of different link prediction methods in the military network may change dramatically when noise exists, and R value is such an index to quantify the

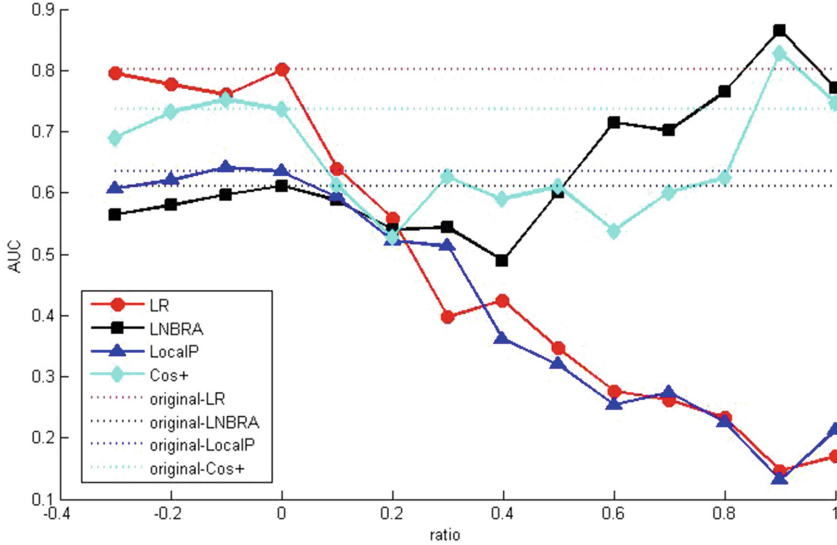


Fig. 6. The dependence of link prediction algorithms' accuracy(AUC) on $ratio$ in the military network. The listed link prediction algorithm are LR , $LNBRA$, $LocalP$, $Cos+$. Dashed lines represent the AUC of these prediction algorithms in the clean network (i.e., the network without any noisy or missing links). $ratio < 0$ represents the missing link case and $ratio > 0$ stands for the noisy link case. Each data point is averaged over 100 independent implementations.

different decay speed of AUC , which will be discussed later; (2) randomly removing links are less destructive than randomly adding link given the same $|ratio|$ value. Taking the $Cos+$ index as an example, adding 30% noisy links will decrease AUC from 0.7363 to 0.6260, the drop is 0.1103, while removing the same amount of random links will make the AUC be around 0.6906, the drop is 0.0457. This is on the contrary to results in ref. [21], and the possible explanation may be that for the complex military organization, mistaken information (noisy links) may be more misleading (destructive) than missing information (missing links); (3) LR performs the best as the ratio ranges from -0.3 to 0.2 , which means our method is the most robust and efficient one under the condition of small noise.

Next, we utilize R index defined in formula (11) to measure the algorithm robustness when links are randomly added or removed from the training set, and R depends on $ratio$ apparently. In Fig. 7, we investigate the effects of $ratio$ on R . And also we just show LR , $LNBR$, $LocalPath$ and $Cos+$ for a clear illustration.

It can be observed from Fig. 7 that: (1) the differences between algorithms' R values increase with $ratio$ when $ratio$ is positive, indicating the different decaying speed of different algorithms' robustness; (2) randomly adding spurious links is more destructive to the algorithms' robustness, take LR as an example, given the same $|ratio|$ value, R is 1.056 when $ratio = -0.3$, while 0.8231 when $ratio = 0.3$;

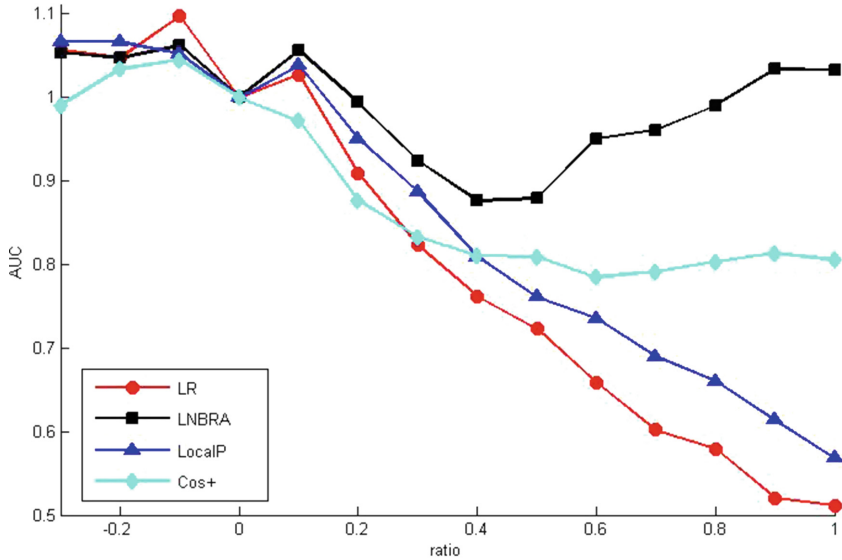


Fig. 7. The dependence of R on $ratio$. The listed link prediction algorithm are LR , $LNBR$, $LocalP$, $Cos+$. $ratio < 0$ represents the missing link case and $ratio > 0$ stands for the noisy link case. Each data point is averaged over 100 independent implementations.

(3) *LR* maintains a comparative higher robustness under small noise environment ($-0.1 \leq \text{ratio} \leq 0.1$).

4 Conclusion and Discussion

This paper tries to address the problem of link prediction in complex military organization network, which is essential for commanders to obtain the qualified intelligence and make the right decisions. Three main contributions are made. Firstly, we measured the nodes' types' effects on their linking behaviors based on the stochastic block model and proved its efficiency empirically. Secondly, we proposed a new link prediction index for complex military organization network, considering both the nodes' types' effect and nodes' structural similarities, and proved it is remarkably superior to all the existent similarity-based indexes, both in predicting missing links and identifying spurious links. Finally, we investigated link prediction algorithms' robustness in the military network under noisy environment, and found that: (1) spurious links are more destructive than missing links for prediction accuracy in military network, which is on the contrary to the results in [21], indicating that mistaken information may be more misleading in military areas; (2) for some indexes, such as *Cos+* and Local Naive Bayes based indexes, their prediction accuracies may even be improved with a certain spurious links existing, and the hidden reason may account for that the random spurious links improve the connectivity of network, and densely connected networks are easier predictable for these methods; (3) Our method performs the best under noisy-free environment, and it still maintains the best accuracy under the condition of small noise, however, as the noise strength increases, its accuracy would be cut down sharply. All in all, *LR* is an efficient link prediction index for complex military organization network, with both high accuracy in predicting missing links and identifying spurious links and robustness under low noisy environment. Since the military area is very sensitive, the intelligence must be carefully artificially checked before we use the algorithm to purify it, which may reduce much obvious noise and leave a network with small latent noise, and that's just our method could still work well on, as a result, the method is practicable in reality.

Since our method is based on the FINC-E model, and FINC-E methodology is also applicable to criminal networks [12], disaster rescue [4], safety culture [18] and social management [16]. Take the business organizations as an instance, the force nodes could be the sales forces and business markets; the intelligence nodes could be the market research and development institutes; and the C2 nodes could be the managers and decision-makers, thus our method could also be applied to these areas for many tasks, such as detecting the underground relationships between terrorists, predicting the potential business markets for decision-makers, and so on.

In the future, we should validate the method in more real military network data, and test its applications in the other social organization areas mentioned above. Besides, since the structure of the military organization is changeable

overtime, link prediction analysis should be considered in the dynamic environment, as a result, we should further study the link prediction in time-dependent military networks.

Acknowledgements. The authors are grateful to the anonymous referees for their insightful suggestions and comments. This research was supported by the National Basic Research Program of China under Grant No. 71471176, No. 71471174 and No. 61303266. All authors acknowledge the National University of Defense Technology.

References

1. Alberts, D.S., Garstka, J.J., Hayes, R.E., Signori, D.A.: Understanding information age warfare. Technical report, DTIC Document (2001)
2. Alberts, D.S.: The Agility Advantage: A Survival Guide for Complex Enterprises and Endeavors. DoD Command and Control Research Program, Washington, D.C (2011)
3. Cares, J.: Distributed Networked Operations The Foundations of Network Centric Warfare. iUniverse, Bloomington (2006)
4. Dekker, A.: Applying social network analysis concepts to military C4ISR architectures. *Connections* **24**(3), 93–103 (2002)
5. Dekker, A.H.: C4ISR architectures, social network analysis and the FINC methodology: an experiment in military organisational structure. Technical report, DTIC Document (2002)
6. Dekker, A.H.: Network topology and military performance (2005)
7. Dekker, A.H., et al.: C4ISR, the FINC methodology, and operations in urban terrain. *J. Battlef. Technol.* **8**(1), 25 (2005)
8. Getoor, L., Diehl, C.P.: Link mining: a survey. *ACM SIGKDD Explor. Newslett.* **7**(2), 3–12 (2005)
9. Hanley, J.A., McNeil, B.J.: The meaning and use of the area under a receiver operating characteristic (ROC) curve. *Radiology* **143**(1), 29–36 (1982)
10. Hayes, R.E.: Measuring command and control (c2) effectiveness. In: MORS Workshop-joint Framework for Measuring C2 Effectiveness. Citeseer, Laurel, MD (2012)
11. Holland, P.W., Laskey, K.B., Leinhardt, S.: Stochastic blockmodels: first steps. *Soc. Netw.* **5**(2), 109–137 (1983)
12. Hutchins, C.E., Benham-Hutchins, M.: Hiding in plain sight: criminal network analysis. *Comput. Math. Organ. Theory* **16**(1), 89–111 (2010)
13. Lin-yuan, L.: Link prediction on complex networks. *J. Univ. Electron. Sci. Technol. China* **39**(5), 651–661 (2010)
14. Lü, L., Zhou, T.: Link prediction in complex networks: a survey. *Physica A* **390**(6), 1150–1170 (2011)
15. Lü, L., Zhou, T.: Link Prediction. Higher Education Press, Beijing (2012)
16. Meyer, M., Zaggel, M.A., Carley, K.M.: Measuring CMOTs intellectual structure and its development. *Comput. Math. Organ. Theory* **17**(1), 1–34 (2011)
17. Shang, M.S., Lü, L., Zeng, W., Zhang, Y.C., Zhou, T.: Relevance is more significant than correlation: information filtering on sparse data. *EPL (Europhys. Lett.)* **88**(6), 68008 (2010)

18. Sharpanskykh, A., Stroeve, S.H.: An agent-based approach for structured modeling, analysis and improvement of safety culture. *Comput. Math. Organ. Theory* **17**(1), 77–117 (2011)
19. Tong, H., Faloutsos, C., Pan, J.Y.: Fast random walk with restart and its applications (2006)
20. Yang, G., Zhang, W., Xiu, B., Liu, Z., Huang, J.: Key potential-oriented criticality analysis for complex military organization based on finc-e model. *Comput. Math. Organ. Theory* **20**(3), 278–301 (2014)
21. Zhang, P., Wang, X., Wang, F., Zeng, A., Xiao, J.: Measuring the robustness of link prediction algorithms under noisy environment. *Sci. Rep.* **6** (2016)

Social Media Processing

5th National Conference, SMP 2016, Nanchang, China,

October 29–30, 2016, Proceedings

Li, Y.; Xiang, G.; Lin, H.; Wang, M. (Eds.)

2016, XIV, 288 p. 87 illus., Softcover

ISBN: 978-981-10-2992-9